



**U.S. Department of Justice**

Criminal Division

*Office of Enforcement Operations*

*Washington, D.C. 20530*

**VIA Electronic Mail**

June 16, 2020

Jonathan Manes, Esq.  
Roderick & Solange MacArthur Justice Center  
160 E. Grand Ave., Sixth Floor  
Chicago, IL 60611  
[jonathan.manes@law.northwestern.edu](mailto:jonathan.manes@law.northwestern.edu)

Request No. CRM-300680988  
Privacy International et al. v. Federal  
Bureau of Investigation, et al., 18-cv-1488  
(W.D.N.Y.)

Dear Mr. Manes:

This is the seventh installment of the Criminal Division's rolling production regarding your Freedom of Information Act request dated September 10, 2018, for certain records pertaining to "computer network exploitation" or "network investigative techniques." Your request is currently in litigation, Privacy International, et al. v. Federal Bureau of Investigation, et al., 18-cv-1488 (W.D.N.Y.). You should refer to this case number in any future correspondence with this Office. This request is being processed in accordance with the interpretation and parameters set forth by defendants in the July 12, 2019, letter to you from Senior Trial Counsel Marcia Sowles, as well as subsequent conversations regarding the Criminal Division's processing of the request.

Please be advised that a search has been conducted in the appropriate sections, and we are continuing to review and process potentially responsive records. After carefully reviewing 540 pages of records, I have determined that 329 pages are responsive to your request and 302 are appropriate for release in full, copies of which are enclosed. Additionally, 27 pages are exempt from disclosure pursuant to:

5 U.S.C. § 552(b)(5), which concerns certain inter- and intra-agency communications protected by the deliberative process privilege and the attorney work-product privilege; and

5 U.S.C. § 552(b)(7)(E), which concerns records or information compiled for law enforcement purposes the release of which would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S.C. § 552(c). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

You may contact Senior Trial Counsel Marcia K. Sowles by phone at (202) 514-4960, by email at [Marcia.Sowles@usdoj.gov](mailto:Marcia.Sowles@usdoj.gov), or by mail at the Civil Division, Federal Programs Branch, 1100 L Street, N.W., Room 10028, Washington, D.C. 20005, for any further assistance and to discuss any aspect of your request.

Although I am aware that your request is the subject of ongoing litigation and that appeals are not ordinarily acted on in such situations, I am required by statute and regulation to inform you of your right to an administrative appeal of this determination. If you are not satisfied with my response to this request, you may administratively appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, 441 G Street, NW, 6th Floor, Washington, D.C. 20530, or you may submit an appeal through OIP's FOIA STAR portal by creating an account on the following website: <https://foiastar.doj.gov>. Your appeal must be postmarked or electronically transmitted within 90 days of the date of my response to your request. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal."

Sincerely,



Amanda Marchand Jones  
Chief  
FOIA/PA Unit

cc: Marcia K. Sowles  
Senior Trial Counsel  
Civil Division, Federal Programs Branch  
1100 L Street, N.W., Room 11028  
Washington, D.C. 20005  
[Marcia.Sowles@usdoj.gov](mailto:Marcia.Sowles@usdoj.gov)

Michael S. Cerrone  
[michael.cerrone@usdoj.gov](mailto:michael.cerrone@usdoj.gov)

Enclosures

**January  
2018  
Volume 66  
Number 1**

United States  
Department of Justice  
Executive Office for  
United States Attorneys  
Washington, DC 20530

James A. Crowell, IV  
Director

Contributors' opinions and statements  
should not be considered an  
endorsement by EOUSA for any  
policy, program, or service

The United States Attorneys' Bulletin  
is published pursuant to  
28 C.F.R. § 0.22(b)

The United States Attorneys' Bulletin  
is published by the  
Executive Office for United States  
Attorneys  
Office of Legal Education  
1620 Pendleton Street  
Columbia, South Carolina 29201

**Editor**  
K. Tate Chambers

**Assistant Editors**  
Nikki Piquette  
Becky Catoe-Aikey  
Brenda S. Mercer

**Law Clerks**  
Gurbani Saini  
Brandy Sanderlin

**Internet Address**  
<https://www.justice.gov/usao/resources/united-states-attorneys-bulletins>

Send article submissions  
to Editor,  
United States Attorneys' Bulletin  
National Advocacy Center  
Office of Legal Education  
1620 Pendleton Street  
Columbia, SC 29201

Cite as:  
66 U.S. Attorneys' Bulletin,  
January 2018

# Emerging Issues in Federal Prosecutions

## In This Issue

<b>Introduction</b> .....	1
By Jeff Sessions, Attorney General of the United States	
<b>Biometric Basics: Options to Gather Data from Digital Devices Locked by a Biometric “Key”</b> .....	3
By Joey L. Blanch and Stephanie S. Christensen	
<b>Mastering eLitigation: How to Organize the Collection, Review, and Production of Large Volumes of Data in Complex Investigations</b> .....	13
By Daniel V. Shapiro and John Haried	
<b>Dismantling an Alien Smuggling Ring: Investigation and Prosecution Challenges for Federal Prosecutors</b> .....	25
By Jason E. Corley and Eric Vincent Carroll	
<b>In Search of Shadows: Investigating and Prosecuting Crime on the “Dark Web”</b> .....	41
By Keith Becker and Ben Fitzpatrick	
<b>Expanding Victim Rights</b> .....	49
By Katharine L. Manning	
<b>When Attorney-Client Communication is Not Privileged: Invoking the Crime-Fraud Exception in Grand Jury Investigations</b> .....	57
By Gretchen C. F. Shappert	
<b>Investigating and Prosecuting Law Enforcement Sexual Misconduct Cases</b> .....	77
By Fara Gold	
<b>Can’t Touch This: Payment Schedules that Prevent Obtaining Defendants’ Assets for Restitution</b> .....	93
By G. Ian Peng	
<b>Marital Privilege in Domestic Violence and Child Abuse Cases in Federal Courts: Exceptions to the Privilege and Compelling Testimony</b> .....	105
By Sasha N. Rutizer	
<b>Coming Soon to a Theater Near You – Motions to Prevent the Cross Examination of Defense Experts</b> .....	117
By James D. Peterson	
<b>Two New Self-Authentication Rules That Make It Easier to Admit Electronic Evidence</b> .....	127
By John M. Haried	

# Emerging Issues in Federal Prosecutions

## In This Issue

**January  
2018  
Volume 66  
Number 1**

United States  
Department of Justice  
Executive Office for  
United States Attorneys  
Washington, DC 20530

James A. Crowell, IV  
Director

Contributors' opinions and statements  
should not be considered an  
endorsement by EOUSA for any  
policy, program, or service

The United States Attorneys' Bulletin  
is published pursuant to  
28 C.F.R. § 0.22(b)

The United States Attorneys' Bulletin  
is published by the  
Executive Office for United States  
Attorneys  
Office of Legal Education  
1620 Pendleton Street  
Columbia, South Carolina 29201

#### Editor

K. Tate Chambers

#### Assistant Editors

Nikki Piquette  
Becky Catoe-Aikey  
Brenda S. Mercer

#### Law Clerks

Gurbani Saini  
Brandy Sanderlin

#### Internet Address

<https://www.justice.gov/usao/resources/united-states-attorneys-bulletins>

Send article submissions  
to Editor,  
United States Attorneys' Bulletin  
National Advocacy Center  
Office of Legal Education  
1620 Pendleton Street  
Columbia, SC 29201

Cite as:  
66 U.S. Attorneys' Bulletin,  
January 2018

<b>Responding to Defense Demands for Government Assistance in Large ESI Criminal Cases</b> .....	139
<b>By John W. M. Claud</b>	
<b>The Resurgence of Denaturalization: The Supreme Court's Decision in <i>Maslenjak</i> and Its Initial Impact on Civil and Criminal Cases Seeking Revocation of U.S. Citizenship</b> .....	149
<b>By Timothy M. Belsan, Aram A. Gavoor, and Joseph A. Marutollo</b>	
<b>International Parental Kidnapping: An Overview of Federal Resources to Assist Your Investigation and Prosecution</b> .....	159
<b>By Jennifer Toritto Leonardo</b>	
<b>Protecting Law Enforcement Peer-to-Peer Investigations</b> .....	167
<b>By Jeffrey H. Zeeman and Joanne C. Pasquarelli</b>	
<b>Transnational Drug Trafficking Act of 2015</b> .....	179
<b>By Stephen Sola, Paul Laymon, and Thomas Johnson</b>	
<b>Prosecuting Federal Hate Crimes</b> .....	191
<b>By Barbara Kay Bosserman and Angela M. Miller</b>	
<b>Note from the Editor</b> .....	237
<b>By K. Tate Chambers</b>	

# Introduction

*Jeff Sessions*

*Attorney General of the United States*

This issue of USA Bulletin, “Emerging Issues in Federal Prosecutions,” provides important information that will better inform all prosecutors and investigators about the new challenges we face on a daily basis. I want to personally write the introduction to stress my support for the USA Bulletin and its mission. Good ideas are essential for skill development for even our most experienced and able practitioners.

A key approach that sets the best professionals apart from their peers is that the best never stop learning. They remain as determined to improve in their sixties as they were in their twenties. This publication is a great tool to help all learn and improve. It engenders excellence and increased productivity. It shares proven ideas and techniques.

I want to ensure that our Department empowers and encourages you to seek excellence and increased productivity. We want to give you guidance on policy, and we want to unleash your creativity and energy. This is the way you will be most fulfilled in your work and the way the goals of the DOJ will be best met. To paraphrase Churchill’s question, “And what is our policy?” For us, the answer is clear. We will use all our resources, personnel, training, skills, and passion to make America a better, more honorable, safer, and more prosperous place. It is not just how many we prosecute and precisely how much time the convicted receive (though these are very important matters), we want to use all our resources and efforts to reduce crime in America.

This “USA Bulletin” provides timely information that covers critical issues such as electronically stored evidence, alien smuggling, criminal discovery, the dark web, victim’s rights, and trial techniques, among other issues. The writers give updates on legal, technological, and legislative changes that will surely benefit all.

My thanks are extended to the editors and writers for their hard work in producing these valuable insights. I am a strong supporter of this periodical.

Page Intentionally Left Blank

# Biometric Basics: Options to Gather Data from Digital Devices Locked by a Biometric “Key”

*Joey L. Blanch*  
*Deputy Chief, Violent and Organized Crime Section*  
*United States Attorney’s Office*  
*Central District of California*

*Stephanie S. Christensen*  
*Chief, Computer Crimes and Intellectual Property Section*  
*United States Attorney’s Office*  
*Central District of California*

## I. Introduction

Increasingly, mobile devices such as smartphones, tablets, and laptop computers play a critical role in everyday life. Mobile devices can contain evidence of communications through email, text message, instant message, and social networking applications. They can contain bank account records, consumer data, health and fitness records, photographs, videos, and evidence of internet activity. This is true for criminals as well as law-abiding citizens, which means that mobile devices can hold a treasure trove of evidence for law enforcement.

Because mobile devices expose so much sensitive and personal data, securing these devices from unwanted intrusion has become a big issue for consumers and companies manufacturing the devices. New security features, designed to protect mobile device users from unlawful intrusion into their devices and data, also protect criminals from lawful, warranted searches. It is therefore critical that prosecutors are aware of these security features and understand how the technology and the law intersect.

## II. What Are “Biometrics”

For years, cellphones have come equipped with a “passcode unlock” feature, requiring a user to type in a numeric or alpha numeric passcode to gain access to the device and the sensitive data inside. A “locked” digital device might mean that the data inside is encrypted and thus cannot be accessed unless unlocked.

An increasingly common feature of digital device security is a “biometric” device lock. In the context of digital devices, “biometrics” generally refers to processes used to identify a person based on physical characteristics, thereby giving them access to and control of the device. This technology includes mechanisms such as fingerprint recognition, facial recognition, retina and iris recognition, and voice recognition to unlock a device and, in many cases, to decrypt data.

### A. Fingerprint Recognition

Apple Inc., Motorola, HTC, and Samsung, among other companies, produce devices that can be unlocked with a fingerprint placed on a fingerprint sensor feature. Each company has a different name for

its fingerprint sensor feature; for example, Apple's is called "Touch ID." Once a user has set up the fingerprint sensor feature in the security settings of the device, the user can unlock the device by placing a finger or thumb on the device's fingerprint sensor. If that sensor recognizes the fingerprint or thumbprint, the device unlocks. Most devices can be set up to recognize multiple prints, so that different prints, not necessarily from the same person, will unlock the device. The presence of a fingerprint sensor on the device makes it easy to tell whether a device has fingerprint unlock capability. Aside from successfully unlocking the device, however, there is no way to tell whether the feature is enabled, and it can be turned on and off by the user. When the registered finger is properly depressed on the sensor, unlocking usually takes two seconds or less.

Manufacturers may include limits on the ability to use a fingerprint or thumbprint to unlock a device. For example, with Apple, the Touch ID feature will not allow access if: a) the device has been restarted or was off and has been turned on; b) the device has received a remote lock command; c) more than forty-eight hours have passed since the device has been unlocked in any fashion; d) the device has not been unlocked with its passcode in six days and also has not been unlocked with Touch ID in eight hours (or less, depending on the operating system installed); or e) five attempts to match a print have been unsuccessful. Other brands have similar restrictions.

## **B. Facial Recognition**

Several hardware and software manufacturers also offer facial recognition security features. As with a fingerprint feature, if the facial recognition feature is enabled, a user can register his or her face to be used to unlock the device. To activate the facial recognition feature, a user must face the device. The device's front-facing camera analyzes and records data based on the user's facial characteristics. The device is then automatically unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Early versions of this feature, for example the one on Samsung's Galaxy S8 and Note 8, could often be defeated by holding up a photograph of the registered face to the device. However, Apple's new "Face ID" feature uses infrared light to scan faces in 3D, so it cannot be tricked by a photograph (although a Vietnamese company has claimed that it can be fooled by a sophisticated 3D model of the registered user's face). The scan and unlock activity is almost instantaneous, occurring in under two seconds. As with fingerprint unlock features, there are often limits on the use of the facial recognition feature to unlock a device. For example, Face ID has limitations similar to those discussed above for Touch ID. Moreover, Face ID may not work if the registered user closes her eyes during the scan.

## **C. Retinal/Iris Recognition**

While not as prolific on digital devices as fingerprint and facial recognition features, both iris and retinal scanning features exist for securing devices/data. The human iris, like a fingerprint, contains complex patterns that are unique and stable, and iris recognition technology uses mathematical pattern recognition techniques to map it using infrared light. Similarly, retinal scanning casts infrared light into a person's eye to map the unique variations of a person's retina blood vessels. A user can register one or both eyes to be used to unlock a device with these features. To activate these features, the user faces the device while the device directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data. The device can then be unlocked if the infrared-sensitive camera detects the registered eye. Both the Samsung Galaxy S8 and Note 8 (discussed above) have iris recognition features. In addition, Microsoft has a product called "Windows Hello" that provides users with a suite of biometric features, including fingerprint, facial, and iris unlock features. Windows Hello has both a software and hardware component, and multiple companies manufacture compatible hardware, for example, attachable infrared cameras or fingerprint sensors to enable the Windows Hello features on older devices.

### **III. Can Law Enforcement Legally Compel Provision of the Biometric Key**

It is not uncommon for law enforcement to have the legal authority to search a mobile device but be unable to conduct the search because the device is “locked.” Where unlocking a device requires a defendant to use a password, compelling the defendant to unlock the device may require the defendant to make a testimonial communication that implicates the Fifth Amendment privilege against compelled self-incrimination.<sup>1</sup> In limited circumstances, however, the “foregone conclusion” exception to the Fifth Amendment may allow the government to require a defendant to produce a device in an unlocked state.<sup>2</sup>

But what if the device can be unlocked by a biometric “key”? Can law enforcement require an individual to place his finger on the sensor? Can a person be compelled to allow her face or eye to be scanned to unlock a device protected by facial, iris or retinal scan features? What legal authority, if any, is required?

#### **A. There is a Strong Argument that the Fifth Amendment Presents No Barrier to Compelling a Biometric Key**

The Fifth Amendment provides that “[n]o person . . . shall be compelled in any criminal case to be a witness against himself . . .”<sup>3</sup> The Fifth Amendment does not, however, proscribe the compelled production of every sort of incriminating evidence. Rather, it “applies only when the accused is compelled to make a Testimonial Communication that is incriminating.”<sup>4</sup> In analyzing whether an act is testimonial under the Fifth Amendment, the Supreme Court has used an analogy—is the act like telling an inquisitor the combination to a wall safe or like being compelled to produce a key to a strong box. Being forced to provide the combination is testimonial; providing a key is not.<sup>5</sup> Biometrics is simply a key based on a person’s physical characteristics.

[T]here is a significant difference between the use of compulsion to extort communications from a defendant and compelling a person to engage in conduct that may be incriminating. Thus, even though the act may provide incriminating evidence, a criminal suspect may be compelled to put on a shirt, to provide a blood sample or handwriting exemplar, or to make a recording of his voice. The act of exhibiting such physical characteristics is not the same as a sworn communication by a witness that relates either express or implied assertions of fact or belief.<sup>6</sup>

The Supreme Court has repeatedly held that the Fifth Amendment does not protect against compelling an individual to exhibit physical characteristics, even if those physical characteristics are

---

<sup>1</sup> See *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F.3d 1335, 1337 (11th Cir. 2012) (reversing order holding the suspect in civil contempt for refusing to comply with a grand jury subpoena requiring him to decrypt hard drives having been granted act-of-production but not derivative-use immunity); *Sec. & Exch. Comm’n v. Huang*, 2015 WL 5611644, at 1–2 (E.D. Pa. Sept. 23, 2015) (compelling passwords would “require intrusion into the knowledge of Defendants”); and *United States v. Kirschner*, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010) (ordering defendant to surrender password requires defendant to divulge mental processes, which is testimonial).

<sup>2</sup> See *United States v. Apple MacPro Computer*, 851 F.3d 238, 248 (3d Cir. 2017) (upholding All Writs Act order compelling defendant to produce devices in an unencrypted state where agents knew that the devices contained child pornography and therefore any testimonial component to the decryption was a foregone conclusion).

<sup>3</sup> U.S. CONST. amend. V.

<sup>4</sup> *Fisher v. United States*, 425 U.S. 391, 408 (1976).

<sup>5</sup> *United States v. Hubbell*, 530 U.S. 27, 43 (2000) (citing *Doe v. United States*, 487 U.S. 201, 210 n. 9 (1988)).

<sup>6</sup> *Hubbell*, 530 U.S. at 34–35.

incriminating. The Fifth Amendment does not protect against compelled production of blood samples,<sup>7</sup> handwriting exemplars,<sup>8</sup> voice exemplars,<sup>9</sup> standing in a lineup,<sup>10</sup> or even wearing particular clothing.<sup>11</sup> The Fifth Amendment’s prohibition on compelled incrimination simply does not apply to the use of a person’s “body as evidence when it may be material.”<sup>12</sup>

This same analysis has been applied to the provision of fingerprints. “[B]oth federal and state courts have usually held that [the Fifth Amendment] offers no protection against compulsion to submit to fingerprinting . . .” because the Fifth Amendment privilege against self-incrimination only prevents the use against an accused of testimonial or communicative evidence obtained from him.<sup>13</sup> Providing one’s fingerprint does not require a person to disclose the contents of one’s mind. For example, the Ninth Circuit has held that “requests by the prosecution for . . . fingerprint evidence from a defendant or a suspect are not prohibited by the Fifth Amendment right against self-incrimination because such evidence is not testimonial in nature.”<sup>14</sup>

Because physical characteristics are not protected by the Fifth Amendment, several courts have held that there is no Fifth Amendment protection against use of fingerprints to unlock digital devices.<sup>15</sup>

While there is not yet significant case law addressing the use of facial recognition, or iris or retinal scanning to unlock a device, the rationale is the same. Further, at least one court has upheld compelled use of a facial recognition unlock feature against a Fifth Amendment challenge.<sup>16</sup>

While the above cases present strong authority and reasoning, prosecutors should beware of the “but cell phones are different” argument stemming from the Supreme Court’s decision in *Riley v. California*.<sup>17</sup> For example, there is a *Riley*-esque feeling among some judges that cell phones are

---

<sup>7</sup> *Schmerber v. California*, 384 U.S. 757, 771 (1966).

<sup>8</sup> *Gilbert v. California*, 388 U.S. 263, 266 (1967).

<sup>9</sup> *United States v. Dionisio*, 410 U.S. 1, 6-7 (1973).

<sup>10</sup> *United States v. Wade*, 388 U.S. 218, 221 (1967).

<sup>11</sup> *Holt v. United States*, 218 U.S. 245, 252-53 (1910).

<sup>12</sup> *Schmerber*, 384 U.S. at 763 (quoting *Holt*, 218 U.S. at 252-53). *See also* *Dionisio*, 410 U.S. at 5-6 (“It has long been held that the compelled display of identifiable physical characteristics infringes no interest protected by the privilege against compulsory self-incrimination.”).

<sup>13</sup> *Schmerber*, 384 U.S. at 764.

<sup>14</sup> *Commonwealth of N. Mariana Islands v. Bowie*, 243 F.3d 1109, 1120 n.5 (9th Cir. 2001); *United States v. Sanudo-Duarte*, 2016 WL 126283 (D. Ariz. Jan. 12, 2016) (holding that defendant could be compelled to provide exemplar of his palm prints).

<sup>15</sup> *See* *Matter of Search Warrant Application for [redacted text]*, No. 17 M 85, 2017 WL 4563861, at 4 (N.D. Ill. Sept. 18, 2017) (holding that compelled act of placing finger on device was not an act of communication, and therefore not testimonial); *State v. Diamond*, 890 N.W.2d 143, 151 (Minn. Ct. App. 2017), review granted (Mar. 28, 2017) (holding that compelling a defendant to produce his fingerprint to unlock a cellphone did not require a testimonial communication); *Com. v. Baust*, 89 Va. Cir. 267 at \*4 (2014) (holding that defendant could be compelled to provide his fingerprint in order to unlock phone); *State v. Stahl*, 206 So. 3d 124, 135 (Fla. Dist. Ct. App. 2016) (“Compelling an individual to place his finger on the iPhone would not be a protected act; it would be an exhibition of a physical characteristic, the forced production of physical evidence, not unlike being compelled to provide a blood sample or provide a handwriting exemplar.”).

<sup>16</sup> *See* *United States v. Stephen Adams*, No. 15-CR-410, ECF No. 56 (S.D.N.Y. Dec. 22, 2015) (incorporating by reference the reasons stated in the government’s brief in denying motion to quash grand jury subpoena commanding defendant to appear so that the phone could be unlocked using the facial recognition function).

<sup>17</sup> *Riley v. California*, 134 S.Ct. 2473, 2494-95 (2016) (holding that, in general, law enforcement may not search a cell phone seized from an arrestee without a warrant).

“different” and therefore the Fifth Amendment analysis regarding compelled use of fingerprints on cell phone should also be different than the compelled use of fingerprints in other contexts.<sup>18</sup>

## **B. The Best Practice is to Compel Through Legal Process**

Having determined that compelled use of biometric technologies does not implicate the Fifth Amendment, the question becomes: by what process, if any, should a suspect be compelled? For practical and prophylactic reasons, the answer is often: specific language in the same search warrant that authorizes search and seizure of the digital device.

It can be argued that under certain circumstances no additional legal process is required to seize the biometric key to unlock a lawfully seized device. In *United States v. Dionisio*, the Supreme Court held that the Fourth Amendment prohibition against unreasonable search and seizure applies only where identifying physical characteristics are obtained as a result of unlawful detention of a suspect (or when an intrusion into the body, such as a blood test, is undertaken without a warrant).<sup>19</sup> Even when a suspect is transported against his will to a police station and fingerprinted, a warrant is not required as long as there is reasonable suspicion that the person committed a crime. As the Supreme Court explained in *Hayes v. Florida*, “[t]here is thus support in our cases for the view that the Fourth Amendment would permit seizures for the purpose of fingerprinting, if there is reasonable suspicion that the suspect has committed a criminal act, if there is a reasonable basis for believing that fingerprinting will establish or negate the suspect’s connection with that crime, and if the procedure is carried out with dispatch,” meaning swiftly and efficiently.<sup>20</sup>

Further, if compelled use of the biometric unlock feature occurs during execution of a search warrant (an often-occurring scenario), there is ample case law in support of brief detentions of occupants of a search location.<sup>21</sup>

Holding up a phone to scan someone’s face or eye requires no physical contact with the person, and even having a suspect depress her finger on a sensor (or doing it for her) will likely require minimal contact. Additionally, because biometric unlocking is by design incredibly fast, there is no doubt that compelled use would be done “with dispatch.” Thus, under the right circumstances (e.g., where the device is lawfully seized and law enforcement has lawful contact with a suspect with whom they have reasonable

---

<sup>18</sup> See, e.g., *In re Application for a Search Warrant*, 236 F. Supp. 3d 1066, 1073 (N.D. Ill. 2017) (rejecting search warrant language compelling fingerprint unlock reasoning that “[w]ith a touch of a finger, a suspect is testifying that he or she has accessed the phone before, at a minimum, to set up the fingerprint password capabilities, and that he or she currently has some level of control over or relatively significant connection to the phone and its contents”); *In the Matter of the Search of: The Single-Family Home and Attached Garage located at [redacted]*, No.17-M-85, 2017 WL 4563870, at 7 (N.D. Ill. Feb. 21, 2017) (finding that “the government’s position that the compelled act may be categorized as physical and so is not testimonial under the Fifth Amendment has only superficial appeal”), *overruled by In the Matter of the Search Warrant Application for [redacted text]*, No. 17-M-85, 2017 WL 4563861, at 4 (N.D. Ill. Sept. 18, 2017).

<sup>19</sup> *Dionisio*, 410 U.S. at 4.

<sup>20</sup> *Hayes v. Florida*, 470 U.S. 811, 817 (1985). See also *United States v. Garcia-Beltran*, 389 F.3d 864, 868 (9th Cir. 2004) (“[T]he Court has reaffirmed the principle that the Fourth Amendment does not permit admission of fingerprint evidence resulting from a seizure without reasonable suspicion”; *but cf.* *Davis v. Mississippi*, 394 U.S. 721, 727-28 (1969) (holding that warrantless “dragnet” investigatory “[d]etentions for the sole purpose of obtaining fingerprints are no less subject to the constraints of the Fourth Amendment. It is arguable, however, that, because of the unique nature of the fingerprinting process, such detentions might, under narrowly defined circumstances, be found to comply with the Fourth Amendment even though there is no probable cause in the traditional sense.”).

<sup>21</sup> See *Michigan v. Summers*, 452 U.S. 692, 705 (1981) (a valid search warrant implicitly carries with it the limited authority to briefly detain the occupants on, or in the immediate vicinity of, the premises while the search is being conducted); *United States v. Broussard*, 80 F.3d 1025, 1033 (5th Cir. 1996) (holding that 10-to-15-minute detention of occupant was reasonable while agents searched occupant’s residence pursuant to valid search warrant).

suspicion of having committed a crime) there is an argument that no specific legal authority is necessary to compel the biometric key. However, what if the suspect refuses to leave his house such that law enforcement lawfully cannot access him within the time limits of the feature without legal process, or refuses to open her eyes to allow for the facial or eye scan? What if the user of the phone is not believed to have committed criminal activity, but her phone nevertheless contains evidence of a crime? Can she be compelled without legal process?

## 1. Subpoenas and All Writs Act Orders

Where further legal authority is necessary or convenient, because no warrant is required, both subpoenas and All Writs Act orders have been used successfully to compel the use of biometric unlock features for devices that were already in law enforcement custody.<sup>22</sup>

However, these tools have limited utility where use of the feature is time-limited (e.g., Touch ID and Face ID) as briefings and hearings on motions to compel or quash can easily render the issue moot.<sup>23</sup>

Thus in many cases for practical and prophylactic reasons, the best practice is to seek authorization to compel biometric unlock in the same search warrant (whether for a person or for a place) that seeks authorization to search the digital device.

## 2. Search Warrants

A search warrant is based on probable cause, which is a higher standard than reasonable suspicion, and obtaining a search warrant is certainly more burdensome than obtaining and serving a grand jury subpoena. As a practical matter, however, where there is probable cause sufficient to seize the digital device, there is probable cause sufficient to seize “the key” to that device in the form of a person’s fingerprint or facial features, similar to provisions in a warrant to seize other keys.<sup>24</sup> Therefore, when seeking a search warrant that establishes probable cause to search a digital device, it is a simple matter to include a request for authorization to seize the biometric key that will enable that search.

An argument could be made that where law enforcement has obtained a warrant to search and seize a digital device and to seize its key, no additional authorization is required in the warrant to compel biometric unlock. In *Dalia v. United States*, the Supreme Court held that a warrant must describe with particularity the place to be searched and items to be seized, but not the manner of execution.<sup>25</sup> “[T]he details of how best to proceed with the performance of a search authorized by warrant” are “generally left to the discretion of the executing officers.”<sup>26</sup> Furthermore, executing officers “may find it necessary to

---

<sup>22</sup> See *Apple MacPro Computer*, 851 F.3d at 244-45 (3d Cir. 2017) (upholding use of All Writs Act order in furtherance of search warrant over challenge by defendant that the government was required to use a grand jury subpoena); *United States v. Stephen Adams*, No. 15-Cr-410, ECF No. 56 (S.D.N.Y. Dec. 22, 2015) (incorporating by reference the reasons stated in the government’s brief in denying motion to quash grand jury subpoena commanding defendant to appear so that the phone could be unlocked using the facial recognition function).

<sup>23</sup> See, e.g., *id.*; *Application of U. S. of Am. for an Order Authorizing an In-Progress Trace of Wire Commc’ns over Tel. Facilities*, 616 F.2d 1122, 1132-33 (9th Cir. 1980) (“[W]e believe that a telephone company whose cooperation in electronic surveillance is sought [pursuant to an All Writs Act order] should be afforded reasonable notice and an opportunity to be heard prior to the entry of any order compelling its assistance.”); *Application of U. S. of Am. for Order Authorizing Installation of Pen Register or Touch-Tone Decoder & Terminating Trap*, 610 F.2d 1148, 1157 (3d Cir. 1979) (“We conclude that due process requires a hearing on the issue of burdensomeness before compelling a telephone company to provide tracing assistance.”).

<sup>24</sup> See *United States v. Shi*, 525 F.3d 709, 731-32 (9th Cir. 2008) (authorizing seizure of keys and identification cards to show indicia of ownership); *United States v. Cowan*, 674 F.3d 947, 953 (8th Cir. 2012) (search warrant included seizing keys as indicia of occupancy or ownership of the premises).

<sup>25</sup> *Dalia v. United States*, 441 U.S. 238, 255 (1979).

<sup>26</sup> *Id.* at 257.

interfere with privacy rights not explicitly considered by the judge who issued the warrant.”<sup>27</sup> Subsequently, the “manner in which a warrant is executed is subject to later judicial review as to its reasonableness.”<sup>28</sup> Applied to biometric devices, *Dalia* can be used to argue that specific approval from a court is not necessary in order to use a fingerprint/face/eye to unlock a lawfully seized device during execution of a warrant.

*Dalia*, however, suggests that the more prudent approach is to obtain that specific authorization in the warrant. *Dalia* addressed whether the Fourth Amendment required a Title III electronic surveillance order authorizing interception of all communications occurring inside a particular location, including a specific authorization to covertly enter the location(s) in question to install the surveillance equipment.<sup>29</sup> While the Court did find that explicit authorization of the entry was not constitutionally required, the Court nevertheless advised that in the future the “preferable approach” was for government agents “to make explicit to the authorizing court their expectation that some form of surreptitious entry will be required to carry out the surveillance.”<sup>30</sup> Given the strong privacy interests involved in searching digital devices, notifying a court and getting judicial approval of the planned method of executing the warrant is very much the “preferable approach.”

A warrant seeking authorization to compel biometric unlock will be strongest when it both provides probable cause to believe that devices with biometric lock features may be present on the person or premises to be searched, and limits the persons who may be tested. Regarding the devices, at least one court has rejected a search warrant with fingerprint unlock language, in part for failure to establish that any Apple devices would be at the premises.<sup>31</sup> The presence of such a device might be established through financial records (showing purchase), surveillance (showing possession), virtual surveillance (showing social media posts discussing, picturing, or making use of a device with biometric unlock capabilities), or user-agent string capture from 2703 process (perhaps showing use on Apple hardware or browser). And if this fails, consider crafting this portion as an anticipatory warrant, with the triggering condition being the presence of a device capable of being biometrically locked.

Regarding the number of persons subject to compulsion, the same magistrate judge who was concerned about the lack of proffered facts pointing to Apple devices was also concerned with the lack of facts discussing who might be present at the target premises and how broadly the “forced fingerprint” order might apply.<sup>32</sup> In contrast, in *In the Matter of the Search of: The Single-Family Home and Attached Garage*, the court considered a government request for a warrant to search a single-family home for evidence of child pornography offenses.<sup>33</sup> In that warrant, the government sought authorization to test the fingerprints of four specifically named individuals—individuals who were associated with the residence, a father, mother, and their two adult sons—to the Touch ID sensors of any Apple devices found. While the court expressed concerns that the government had “no information as to whether Apple devices will be found” at the search location, and “if so, to whom they belong,” the court nevertheless found that the government’s request did not present the same Fourth Amendment concerns it felt would be raised should the government have requested to test the fingerprints of *all* individuals found at the residence.<sup>34</sup>

---

<sup>27</sup> *Id.*

<sup>28</sup> *Id.* at 258.

<sup>29</sup> *Id.* at 241.

<sup>30</sup> *Id.* at 259 n.22.

<sup>31</sup> See *In re Application for a Search Warrant*, 236 F. Supp. 3d at 1068.

<sup>32</sup> *Id.*

<sup>33</sup> *In the Matter of the Search of: The Single-Family Home and Attached Garage*, No.17-M-85, 2017 WL 4563870, at 1.

<sup>34</sup> *Id.* at 2. (While the court ultimately denied the government’s request on Fifth Amendment grounds, that holding was overruled by *In the Matter of the Search Warrant Application for [redacted text]*, No. 17 M 85, 2017 WL 4563861, at 4).

Accordingly, where possible, try to identify persons who may be at the premises and limit the request to those individuals whom the agents have cause to believe may be a user of the seized phone bearing the unlock feature. This would, for instance, exclude the hapless pizza delivery person standing in the doorway, whose face, eyes, or fingers are plainly unlikely to be the key to unlocking the evidence-containing device.

The more narrowly tailored the request is, the more likely it is to be granted, and later upheld.<sup>35</sup>

### **C. Practical Tips for Executing the Search Warrant**

Once court authorization to test individuals for biometric unlock is granted, prosecutors should communicate with the agents to ensure that the warrant is executed in a manner least likely to suggest that the act of unlocking a device is testimonial. For instance, agents should not ask suspects to choose a device to “unlock,” an act that suggests an admission of ownership or control over that device. To remove any suggestion that the target was compelled to make any volitional—and thereby testimonial—act, agents should specifically compel/instruct the suspects as to which fingers to put on the device or eye to open for scanning. It may be the best practice for the agent to physically pick up the suspect’s hand and depress his finger/thumb to the sensor, one at a time, just as if they were taking the suspect’s fingerprints by old-fashioned ink on paper. Even better, seek the suspect’s voluntary cooperation/consent to unlock the phone. Alternatively, consider whether a ruse could avoid the issue altogether. For instance, allow the suspect to make a call with his or her telephone, and then take the phone once she has voluntarily unlocked it.

Further, prosecutors should talk to the agents in advance to ensure that a plan is in place to protect the evidence on digital devices that are located, seized, and—fingers crossed—unlocked. Beware; most devices have an “auto-lock” feature that will re-lock the phone after a short period of non-use or if the device loses power. Therefore, once the phone is unlocked, immediate steps should be taken to prevent the phone from re-locking or being tampered with. Suggested steps include the following:

- As soon as possible, the device should be placed into “airplane” mode, which counters most attempts to communicate remotely with the device using cellular data or Wi-Fi and tampering with evidence. (Depending on the device and settings, it may even be possible to place the phone into airplane mode before it is unlocked.)
- Access the device settings and place it on “never” lock. On devices where this feature is available, this will disable auto-lock.
- Seize the charging cord and place the device on a battery pack so the device does not run out of power.
- To further avoid remote-wipe commands, put the device in a Faraday bag or box. These containers are designed specifically to block the device from receiving any remote signals.

For some devices, these steps will be sufficient, and the device can then be transported to a lab for forensic examination using a Cellebrite kiosk to “dump” the phone, or other logical or physical extraction methods. Even if the device is not successfully unlocked, the first and last steps should still be employed in the hope that when an exploit is developed, the data will still be present.

If “never” lock is unavailable, however, time will be of the essence and the agent must be prepared to search the device immediately onsite. If no mobile forensic tool is available to “dump” the phone, this will mean manually taking photographs of seizable information.

---

<sup>35</sup> See *United States v. Chris Hood and Abdul Bangura*, No. 1:17-CR-80-AJT, ECF 48 (E.D.Va. July 21, 2017) (denying motion to suppress evidence obtained from an iPhone unlocked pursuant to language in premises search warrant).

Speaking of taking photographs, agents should be aware that Apple devices running iOS 11 (or later) cannot be “dumped” using a forensic tool such as a Cellebrite kiosk without the passcode. In other words, even if the agent biometrically unlocks the iPhone, at least as of the date of this article, the only extraction method for iOS 11 devices, absent a passcode, is by photograph.

## IV. Conclusion

Biometric locks present an opportunity for law enforcement to execute warrants that might otherwise be thwarted by the “going dark” phenomenon. While upholding the Fourth and Fifth Amendments, we can compel biometric keys and capture vital evidence of criminal wrongdoing through full forensic analysis or, at the very least, by photograph.

### ABOUT THE AUTHORS

□ **Joey L. Blanch** is an Assistant United States Attorney in the Central District of California, currently serving as the Deputy Chief of the Violent & Organized Crime Section in Los Angeles. From 2015 to 2016, she was detailed to the Executive Office for United States Attorneys in Washington D.C. as the National Project Safe Childhood Coordinator of the Central District of California, focusing on the prosecution of crimes against children. She was formerly a Deputy Chief in the General Crimes Section, responsible for supervising and training new AUSAs. Ms. Blanch has taught advocacy as an adjunct professor at Loyola Law School and also lectured on subjects related to trial advocacy and child exploitation at various locations across the country.

□ **Stephanie S. Christensen** is an Assistant United States Attorney in the Central District of California, currently serving as the Chief of the Computer Crimes and Intellectual Property Section in the office’s National Security Division. Ms. Christensen is a National Security Cyber Specialist and serves on CCIPS’ CHIP Working Group. In 2015, she received the Federal Bureau of Investigation’s Director’s Award for Outstanding Cyber Investigation for her work on the cyber intrusion at Sony Pictures Entertainment, one of the most destructive cyber-attacks on U.S. soil. She was also part of the four-person litigation team on *In the Matter of the Search of an Apple iPhone*, the encryption litigation arising from the seizure of an iPhone used by a perpetrator of the terrorist attack in San Bernardino, California. She was a law clerk for the Honorable Gary Allen Feess in the Central District of California and for the Honorable Sandra Ikuta on the Ninth Circuit Court of Appeals.

Page Intentionally Left Blank

# Mastering eLitigation: How to Organize the Collection, Review, and Production of Large Volumes of Data in Complex Investigations

*Daniel V. Shapiro*  
*Assistant United States Attorney*  
*District of New Jersey*

*John Haried*  
*Criminal eDiscovery Coordinator*  
*Executive Office for United States Attorneys*

## I. Introduction

The explosion of digital information has increased the complexity of criminal litigation. Cases that used to have paper investigative reports and business records now have cell tower data, emails, text messages, Facebook chats, Instagram posts, surveillance videos, and more. The challenge of managing all of this digital information becomes even more pronounced in complex long-term investigations.

Complex investigations have unique challenges: large volumes of digital evidence, multiple agents and/or prosecutors during the life span of the case, and significant analysis conducted by the investigative team. Every investigation also requires a dual track. You must gather and preserve evidence in its original state so that it can ultimately be admitted into evidence at trial. At the same time, you must also analyze the collected evidence, which frequently requires the original evidence to be processed in some way to make it more easily reviewed and searched. It is crucial to have a strategy for managing your investigation at the outset of the case. This article will discuss strategies to help prosecutors deal with the large volumes of data involved in complex investigations. It will focus on (1) digital case folder organization, (2) the intake and review of evidence, and (3) tips to avoid the over-collection of digital evidence. We also suggest policies and procedures that will help prosecutors investigate complex cases more quickly, efficiently, and in a way that mitigates litigation risk down the road.

## II. The Digital Case Folder

We urge you to keep your case files digitally. In complex investigations, paper files become unmanageable quickly and make it more difficult for multiple members of your team to work on the case at the same time. Every subpoena return, responsive search warrant record, and other documentary evidence and report should be stored on the computer network of the United States Attorney's Office (the "Digital Case Folder"). Evidence must be added to your Digital Case Folder on a rolling basis as it comes in. Your team cannot analyze evidence if you do not have a copy of it or it exists only on a CD or hard drive in your file cabinet. You should maintain physical copies of court documents with original signatures or certified court documents, but the rest of your file should be entirely digital. The original copy of a grand jury subpoena return or search warrant return should ultimately be maintained in accordance with the policies of your district. If a piece of evidence is too large to copy to the Digital Case

Folder or host in-house at the United States Attorney’s Office, a plan must be made to store, process, and review the evidence. Options include using the Litigation Technology Service Center, an outside vendor, or working with the investigative agency to process and host the data.

Organize your Digital Case Folders in a logical and consistent way. We suggest that you name your Digital Case Folders using a consistent syntax that includes the USAO number in the folder name. Create a default folder structure to use for all of your cases (or all cases of a certain type) and start using it from the beginning of each case. A sample Digital Case Folder (with some example sub-folders) is set forth below:

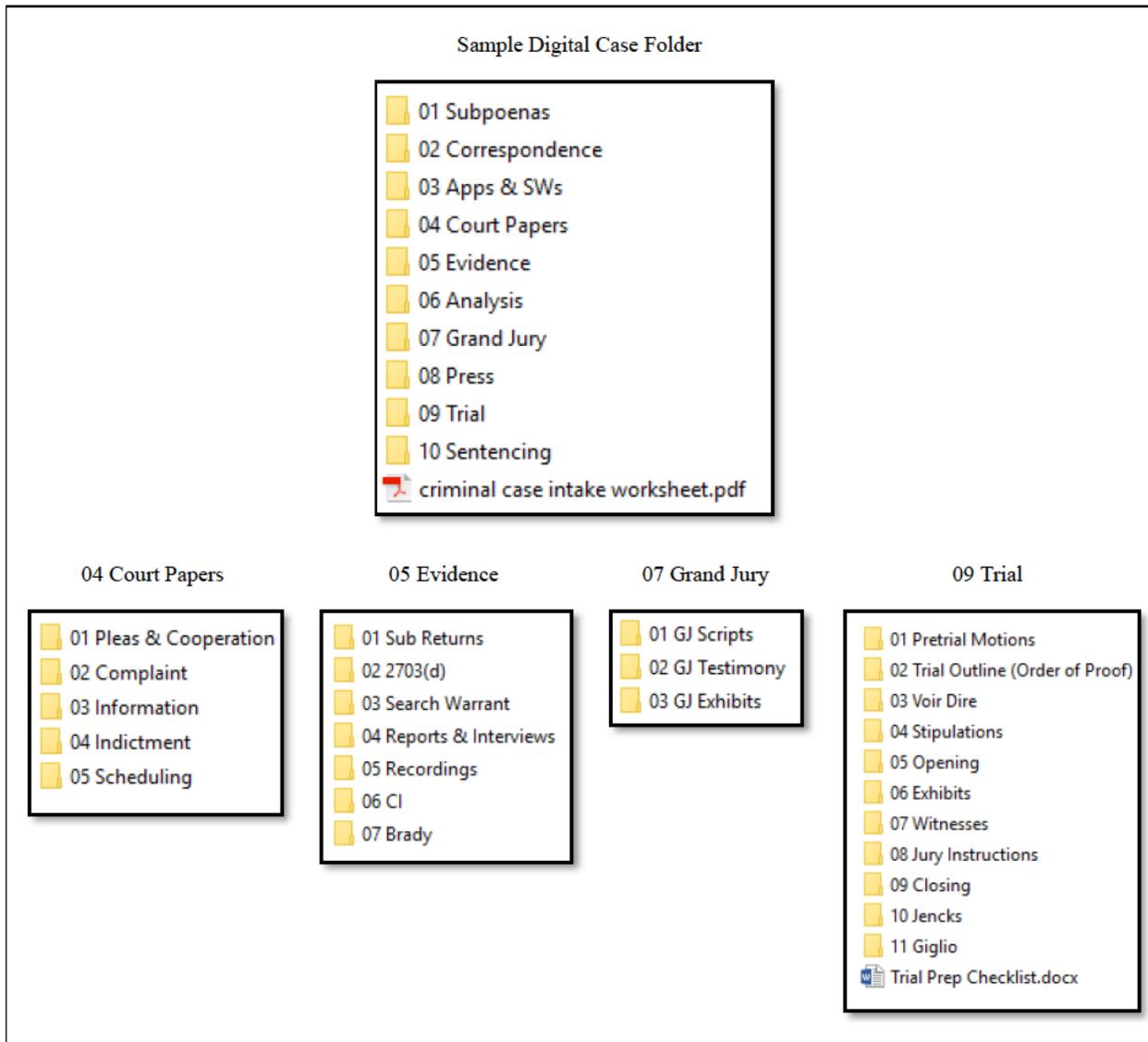


Table 1: Sample Digital Case Folder

Make sure that your Digital Case Folder resides at a location on the network where the rest of your team at your office will have access to it and where supervisors and successor prosecutors would expect to find it. This organization enables legal assistants, paralegals, analysts, and investigators to more effectively work on the case and ensures transitions that are more efficient when members leave and join the investigative team. It also aids in the production of discovery, as further discussed below.

If your district has adopted digital grand jury subpoenas, use them to avoid unnecessary printing and scanning. In cases involving hundreds of subpoenas, this will save a significant amount of time. If you need to restrict access to the Digital Case Folder, speak with your IT staff to limit access.

### III. Evidence Intake and Analysis

Most complex investigations have at least five fundamental litigation needs:

1. A method for storing, organizing, and tracking incoming information.
2. A means of converting incoming information from its raw state—paper, native files, PDFs, subpoena returns, etc.—into an electronic format that your evidence review software can handle.
3. Efficient review of voluminous information using evidence review software.
4. A method for organizing the important facts, hot documents, key witnesses, critical investigative reports, and important transcripts that comprise the core of your investigation.
5. A record of what you produced to the opposing party as discovery.

Each of these five needs is addressed below.

#### A. Storing, Organizing, and Tracking Incoming Information

The starting point is knowing what you have. If you want to understand just how much trouble you can get into by failing to inventory what your investigation has collected, just read *United States v. Pedersen*<sup>1</sup> and *United States v. Toilolo*<sup>2</sup>.

No prosecutor should assume the burden of managing and organizing a complex investigation without help. Fully employ and leverage the support staff of paralegals and legal assistants that work with you. Involve them in the organization of your case and the intake of evidence. For large cases, consider having subpoenas returnable to a paralegal at the United States Attorney's Office instead of directly to an investigative agency. The paralegal can then serve as the central point at which subpoenas are (1) received, (2) copied or scanned to the Digital Case Folder, (3) distributed to the investigative agency, and (4) provided to litigation support for processing to be loaded into a review platform.

To prepare for discovery obligations, you should keep a separate area of your Digital Case Folder for pristine copies of the grand jury subpoena returns and other evidence received in your case (for example, the "05 Evidence" subfolder discussed above). Any analysis of that evidence should be conducted on a review platform or using a copy of that evidence in another part of the Digital Case Folder. When it comes time to produce discovery in the case, you will already have a complete set of subpoena returns and other evidence to turn over.

Track your subpoenas using a numbering system that corresponds to the folders where you store the subpoena returns. First, number your subpoenas using the USAO number for the case and the subpoena number. Each page of your subpoena and any attachments should contain the USAO number and subpoena number so that when you receive back subpoena returns that do not reference any subpoena number, but include a business record certification, you will still be able to associate it with a case.

---

<sup>1</sup> *United States v. Pedersen*, No. 3:12-CR-00431-HA, 2014 WL 3871197 (D. Or. Aug. 6, 2014) (complex case with discovery from multiple law enforcement agencies. "[T]he government mishandled this case badly. It failed to fulfill its discovery obligations . . .").

<sup>2</sup> *United States v. Toilolo*, 666 F. App'x 618 (9th Cir. 2016) (government's handling of discovery was "sloppy, inexcusably tardy, and almost grossly negligent[;]" jury instructed on government's misconduct.).

Second, keep a “subpoena returns” folder in your Digital Case Folder organized with folders with the subpoena number and the entity that produced the records, i.e., 001-Citibank. Use leading zeros to ensure that the folders will sort properly, and if you think there may end up being more than 100 subpoenas in the case, use at least two leading zeros.

A successful intake log requires planning and dogged execution. Before your evidence starts coming in, plan what information you will log and who will be responsible for preparing the log. An intake log can be a simple spreadsheet:

Date Rec'd	Rec'd From	Rec'd By	Source / Obtained From	Description	Format
11/20/2014	IRS Agent Harold Crick	Jamaal Jones	GJ Sub #14-472	Wells Fargo records for account xxx-5810	paper
11/22/2014	DEA SA HSchrader	Jamaal Jones	DEA disk 14	Photos - search warrant executed at 124 S Main	.jpeg
11/28/2014	Google	Sally Smith	Google	2703(d) order for getrichnow@gmail.com	.pst

Table 2: Simple Intake Log

Adding a few columns can make a simple intake log more useful:

Label / ID	Quantity	Storage Location	Contains Contraband	Special Handling Instructions	General Notes
FBI thumb drive 14-209	1	FBI – evidence room	<input checked="" type="checkbox"/>	Needs redaction of CI info	Emailed agent. Contains contraband CP.
Seagate 500 GB ex HD - #4857-MBD	1	USAO – media storage vault – bin #3429-C	<input type="checkbox"/>	Surveillance video in a proprietary format	Need to convert for discovery.

Table 3: More Intricate Intake Log

We recommend using CaseMap or Excel for intake logs. Using those tools, you can easily sort and search information, add custom columns or hide columns as needed, create separate spreadsheets for main categories (grand jury subpoenas, search warrants, 2703 orders, etc.), and link each item to its supporting documents (subpoenas, law enforcement records, photos), etc. We do not recommend using Word because CaseMap and Excel offer features that are more robust and can readily handle more items.

## B. Processing Raw Incoming Information

Once your evidence starts to come in, you need an organized approach to manage and review it. This frequently means using a software tool for efficient review of voluminous documents and other information, as well as software tools to help manage key information. If you are going to use document review software such as Eclipse SE, Relativity, or a similar software, then the incoming raw electronically stored information (“ESI”) and paper records must be “processed” to make them usable by the review software. DOJ uses several software tools for processing, including eScanIT, LAW PreDiscovery, Nuix, and similar commercial products. During 2018, EOUSA will deploy Nuix to all United States Attorney Offices and provide training.

Processing software extracts metadata and text from raw ESI. For example, processing software extracts from a collection of emails their metadata—the date sent, sender, recipient, subject, and attachments, as well as the message’s text content—and stages that information for loading into review software. That makes it possible for the document review software to give you fast and accurate search results, even from thousands or millions of records. The end product of processing software is a package of instructions—called a load file—that tells the computer what, how, and where to stage your data to make it possible for you to use the powerful features of Eclipse and Relativity.

## **1. Deduping**

Processing software can streamline the review process of certain types of evidence by eliminating duplicative files (commonly called “deduplication” or “deduping”), but you should proceed with caution. For example, processing software can detect and segregate out exact duplicates of files. This can make your search more efficient when reviewing, say, 200,000 corporate emails; otherwise, your word search for “sales incentives” will return 10,000 copies of the same quarterly management motivation email sent to all employees. Similarly, processing software can perform “near-deduplication,” which means culling out different file types with the exact same content, for example, the Word and PDF versions of the same document. Reducing the number of hits that are merely duplicates of each other makes your searches and review more efficient. Deduplication is most beneficial when you receive a production of email from a company that includes the email accounts of several employees and that may contain many copies of the same emails. It can also be useful to dedupe when an email provider produces both a preserved copy of an email account and the current contents of that account.

However, the burden in criminal cases to prove an individual defendant’s knowledge and mens rea may make it important to know all of the accounts, devices, and locations where an important document was found. You should be aware that deduplication may end up removing copies of an important document from one set of evidence if another copy is found somewhere else in your deduped data (although they will remain in your pristine, original copy of the data). In addition, filter reviews sometimes require a filter attorney to turn over every document that hits on certain keywords to defense counsel. Deduplication may have removed additional copies of documents that hit on those keywords. For these reasons, we advise caution before deduping your entire investigative database or deduping across sources of documents, i.e., deduping multiple email accounts or electronic devices against each other.

## **2. De-NISTing**

Processing software also can segregate out irrelevant files obtained from the search of an electronic device, such as the application files for computer programs like Microsoft Word or Excel, and the operating system files found on a computer. This process is called “de-NISTing.” NIST is an acronym for the National Institute of Standards and Technology. NIST maintains the National Software Reference Library, which lists common computer applications. De-NISTing the files collected from a computer can eliminate files that are irrelevant and makes your searches faster. This process is best used when you are interested in reviewing the contents of devices, as opposed to conducting a forensic examination. (A forensic examination to show who controlled the electronic device would require access to operating system files and applications.)

## **3. Email Threading**

“Email threading” is another means of simplifying your searches. An email collection typically includes many email chains consisting of the original message, many replies and responses, and forwarded versions. Processing software will identify the threads of related emails. Email threading puts email chains into chronological order and groups related emails together, thereby improving the speed, accuracy, and completeness of your review. In short, processing software can both cull your data set and focus your review on relevant information.

## **4. Optical Character Recognition (OCR)**

When processing paper records to a digital file, processing software creates a static image of the record in a TIFF (Tagged Image File Format) or PDF, together with the paper document’s text obtained by OCR (optical character recognition). This enables computerized word searching, quicker filter review, and easier storage and exchange. However, it is important to note that text obtained by OCR is roughly eighty to ninety percent accurate, which is poor compared to the 100 percent accuracy of text extracted

from ESI. Nonetheless, converting paper records to a digital format permits faster, more efficient, and more complete review compared to review by human eyes on paper.

## **5. Custodians**

There are certain differences between civil and criminal litigation that must be kept in mind when processing data. Processing and document review tools are generally created with civil litigation in mind and not specifically for use in criminal cases. As a result, some of the terminology needs to be adjusted. When processing your evidence, litigation support staff may ask you about the “custodian” field. In a civil litigation where a company has produced voluminous documents, the custodian would likely be the individual to whom the files belong, or from whose office or electronic files the evidence was produced. The vast majority of evidence in a criminal case is not produced this way. We suggest that you typically have the custodian field relate back to the legal process that returned the evidence. For example, the custodian for the Citibank records produced in response to subpoena 001 would simply be 001-Citibank and would match the name of the folder containing those records. For devices obtained from a premises search warrant, the custodian would be the address of the searched premises, e.g., 123 Main Street. Electronic accounts can be organized by the name of the account, e.g., johnsmith@gmail.com. This will also assist you in determining where the evidence originated from when you are reviewing it in your document review platform.

## **6. Discovery Considerations**

You must prepare to be flexible in how you will ultimately produce discovery. Criminal cases differ from civil cases because the judge and defense counsel are unknown until the later phases of an investigation, or until you charge the case. As a result, the preferences of the judge and defense counsel with respect to discovery are also unknown. Processing all of your data, without maintaining an organized complete set of your original data, could be a mistake when defense counsel ultimately asks you for copies of the original evidence you collected.

In addition, processed data is not identical to your original data. It may have been changed during processing and some information may have been removed. For example, depending on the settings used during processing, an email that has been processed may not contain the full detailed header information about all of the computer servers that the email passed through before it was ultimately delivered. If this is important information for your investigation, you should make sure the full email header is extracted during processing. In addition, during discovery you may want to make available copies of the original evidence you received.

## **C. Software Tools for Reviewing Evidence**

At present, USAO litigation teams have two choices for evidence review: Eclipse SE or Relativity. Prosecutors in the other litigating components have different software options.

The document review tools available to United States Attorneys’ Offices will help you efficiently execute critical tasks:

- View documents: You can view native files or processed images.
- Identify relevant documents and cull out irrelevant documents: You can cull documents by date range, source, topic, or other characteristics.
- Sort by characteristics: You can sort by date, author and recipient, document type, or other information.
- View, code, and tag: You can view documents (for example, business records, investigative reports), and tag documents (such as hot doc, the issue or witness they relate to, etc.).

- **Sophisticated searching:** You can search across the different documents in your collection—business records, reports, emails, transcripts, spreadsheets—to identify similar characteristics across data types, much like Westlaw allows you to search for terms and ideas across its information sources. You can also search within searches and by document tags.
- **Highlight, annotate, and redact:** You can record your value-added assessment of individual documents.
- **Track and produce:** You can track when and how documents were received and produced as discovery, and create discovery productions in various formats.

It is important to note that to get the most out of document review software, you should request that electronic information be provided to you in either (1) native format (with original metadata), so that it can be processed into a format that Eclipse SE or Relativity can handle, or (2) load files with associated text and TIFF images that can be loaded directly into Eclipse SE or Relativity. You should involve your litigation support technologist early so that they can assist you in navigating the best way to gather and process electronic information so that it is usable.

Eclipse SE allows you to manage your case within your USAO, with help from your litigation support technologist, paralegal, and systems manager. All of your data will be processed and hosted locally at your USAO. Your USAO's practices and procedures with respect to eDiscovery processing, loading, and productions will continue to govern how your case is supported. Access to Eclipse SE for case team members outside of your USAO requires producing a copy of the database with a stand-alone viewer. This production will be static and will not include any information added to the database after the stand-alone copy is created.

Relativity is a robust document review platform that can handle very large cases. Relativity offers advanced analytical searching tools, including concept searching and “find similar” searches, both of which can be more effective than searches for specific terms. It is web-based, meaning your documents reside on a centralized group of servers, and you can access and review them via a web portal. USAOs have access to Relativity through the Litigation Technology Service Center (LTSC), located in Columbia, South Carolina, which can host Relativity databases that are in the range of low single-digit terabytes in size. Data must be sent to the LTSC, where it is processed. Investigative agencies can be given access to the Relativity web portal to access the most up-to-date version of your data. Because the LTSC services all of the districts in the country, individual USAOs have less control over the priority and order in which data is processed. If you want to know whether the LTSC can host your case, talk with your litigation support technologist.

## **D. Software Tools for Developing Your Case: CaseMap**

CaseMap is a digital trial notebook. It helps you organize what is important: the key facts, documents, witnesses, issues, questions, and legal research. CaseMap is a set of interconnected spreadsheets that hold just your key information about facts, people, documents, issues, questions, and legal research. Importantly, you add to the CaseMap file only what information you decide will serve your needs. It is completely customizable. CaseMap helps you create a list of hot documents that you can turn into an exhibit list; an outline of factual and legal issues for charging, motions practice, and trial; a log of subpoenas issued and returned; a file of key case law, statutes, and regulations; and a To-do list. Most importantly, CaseMap is not extra work. It is a more efficient way of capturing the work you are already doing in other ways. If you start putting your work product into CaseMap from the outset, then it is easy and efficient. That means using CaseMap to preserve your thinking about what is critical to building your case—your facts, witnesses, documents, other evidence, issues, and legal research.

CaseMap’s fact spreadsheet: The chronology of important facts in your case should (1) refer back to the source evidence that proves the fact, and (2) record the legal process that you used to obtain the evidence. The chronology contains the facts that prove your case. The source documents are what you will use to prove your facts. The legal process used to obtain the evidence will lead you to witnesses that will lay the foundation for introducing the evidence at trial. In CaseMap, the items in the “source(s)” column, below, with the dotted underline are linked from this spreadsheet to the actual electronic file proving the fact.

Date & Time ▲	Fact Text ↻	Source(s) ↻
Thu 02/14/1929 9:30 a.m. CT	Al Capone made a phone call about money from his home.	<u>FBI0001923</u> - house photo
Thu 02/14/1929 11:40 a.m. CT	2 men dressed as Chicago Police enter 2122 North Clark Street along with 2 men in street	JonesP 302
Thu 02/14/1929 11:43 a.m. CT	Neighbors in vicinity of 2122 North Clark Street hear loud gun fire.	JonesP 302
Thu 02/14/1929 11:46 a.m. CT	Neighbors see 2 police with weapons drawn on 2 men in street clothes exit 2122 North	JonesP 302
Thu 02/14/1929 12:05 p.m. CT	Police and ambulances arrive at 2122 North Clark Street and find the bodies of 6 dead men	<u>FBI0012003</u> <u>FBI0012004</u>
Wed 05/15/1929	The FBI conducted the search of Al Capone home in Chicago.	<u>FBI0001999</u>

Table 4: Example of an Electronic File

CaseMap’s document/evidence spreadsheet: CaseMap gives you spreadsheets to organize information about documents and other evidence, and even links to the item itself, as shown in the “linked file” column:

Doc date ▲	Description ↻	Doc Summary ↻	Source of Doc +	Linked File
Fri 10/31/1028	Johnny Welder's hand-written notes from 10/31/1928.	Johnny Welder's notes about job to cut Chicago Bank & Trust alarms with welding	Investigation	 ...\Johnny Weld
Thu 02/14/1929	Photo #1 of Valentine's Day Massacre victims' bodies	Shows bodies of Peter Guseberg, Frank Guseberg, Albert Weinsbank, and Albert...	Chicago PD	 ...\Photo - crim
Wed 04/10/1929	Line Sheet re recorded telephone call from Ronnie...	Johnny Torres and Ronnie Garcia discuss an attempt to sell whisky.	Title 3 Wire Tap	 ...\Line sheet sa
Thu 06/20/1929	USFA Check # 628 to Joe Wimer for \$1,360	Proceeds used by Al Capone to pay trigger men	GJ subpoena 29-111	 ...\Photo - USFA

Table 5: Example of the Linked File Column

CaseMap’s witness/persons spreadsheet: CaseMap gives you a spreadsheet you can customize to organize information about your witnesses:

Full Name ▲	Role In Case ↻	Address ↻	Phone Nu... ↻	Email ↻
Allison Becker	FBI tech who monitored intercepted phone calls.	FBI - Chicago	312.555.9999	cbecker@ic.fbi.gov
Joe Boggart	Lead agent for FBI.	FBI - Chicago	312.555.9999	JBoggart@ic.fbi.gov
Byron Bolton	Bolton claims he was involved in the massacre as a look-out,	Federal Witness Protection	Protected	
Al Capone	Mob boss for gang involved in loan sharking, gambling,	1 Lake Shore Drive, Chicago, IL	312.555.1111	ACapone@gmail.com

Table 6: Example of Customizable Spreadsheet

CaseMap gives you similar spreadsheets to organize your witness questions, legal research, and the issues in your case linked to your evidence. In addition, multiple members of your team can access and work in the CaseMap database at the same time.

## E. Tracking the Discovery Produced

Finally, tracking what you produced helps you ensure you have complied with your discovery obligations and helps you prove that, in fact, you did produce the item that the opposing attorney claims he never received. Several software tools are effective for creating discovery production log: CaseMap, Eclipse SE, Excel, and others. Here are some types of information that help you know what you produced:

Vol. No.	Bates - Begin	Description ↻	Sent to ↻	Prod date	Notes ↻
2	USB0001-00246	USBank records - acct #123456	Jim Bacon (def atty)	Wed 06/11/1930	Password = JON#002*DSC
3	FBI0090-0099	FBI crime scene photos	Anita Gonzales Jim Bacon Ian Nicholas	Tue 07/01/1930	Password = JON#003*DSC
2	LS_000008	Line Sheet re recorded telephone call	Ian Nichols (def atty)	Wed 06/11/1930	Password = JON#002*DSC
1	FBI0012741	Al Capone's FBI booking sheet	Anita Gonzales (def atty)	Fri 05/02/1930	Password = JON#001*DSC

Table 7: Example of Production Tracking

## IV. Seized Electronic Devices

The review of electronic devices searched during an investigation is typically a multi-stage process: (1) seize the device, (2) search the device for material responsive to the search warrant, (3) search the responsive material for potential trial exhibits, and (4) establish the foundation necessary to introduce the potential trial exhibits into evidence at trial. The process of reviewing electronic devices is extremely time- and labor-intensive and should be taken into account when deciding how many electronic devices to seize. The fact that you have probable cause to search a device should not be the end of the

analysis. Don't seize a particular computer or cell phone without a substantial reason. You should conduct a cost-benefit analysis for every electronic device seized. Conducting a forensic review of a single electronic device can take months to complete.

Similarly, as your data grows in size and complexity it consumes more of your time, more of your agent's time, and more of your staff's time. Sensitive information—like personal identification information (“PII”) and attorney-client privileged material—may require time-intensive review procedures, including filter team review. At both ends of your workflow—intake and discovery production—higher data volumes mean your litigation support technologist needs much more time for processing, organization, problem solving, and quality control. Just processing voluminous data can take days or weeks. Data storage space is limited, and moving large data sets can be difficult and time consuming. Collecting unnecessary data will gum up your case. Before collecting by seizure or subpoena, try to learn how much data exists, how it is maintained (file types, etc.), and ways to target important information and avoid unimportant information. If possible, create parameters for collections by date ranges, custodians, subject matter, particular transactions, etc. to streamline the amount of data collected.

Finally, many opposing parties and their attorneys simply do not have the technology, staff, and money to review voluminous discovery efficiently. Criminal defendants in pretrial detention and pro se parties have very limited resources. Hence, when you over-collect data, you may be handing the opposing party persuasive grounds to delay trial and drag out the pretrial phase.

## V. Conclusion

Based on the tips and strategies in this article, we suggest the policies and procedures below to investigate complex cases more quickly and efficiently.

### THE DIGITAL CASE FOLDER

1. Keep a digital copy of all of your investigative files on the network at the United States Attorney's Office.
2. Use standard naming conventions for each case that include the USAO number so others can locate the Digital Case Folder.
3. Use standard folder structures for the Digital Case Folder that are put in place at the beginning of the case.

### EVIDENCE INTAKE & ANALYSIS

1. Assign paralegals to complex investigations early. Don't wait until the discovery or trial phase.
2. Use a system to manage and organize the intake of evidence into the Digital Case Folder and put it in place at the beginning of the investigation.

3. Involve Litigation Support early in your investigation.
4. Process data into an evidence review tool, such as Eclipse SE or Relativity, as you receive it.
5. Make sure you understand and discuss with support staff how you want your evidence to be processed before it happens. Discuss deduping, de-NISTing, email threading, and the types of data to extract.
6. Have a method in place to build a chronology for the case.
7. Track the discovery you produce.

#### AVOID OVER-COLLECTION

1. Even if you have probable cause, don't seize a particular computer or cell phone without a substantial reason.
2. Before collecting by seizure or subpoena, try to learn how much data exists, how it is maintained (file types, etc.), and ways to target important information and avoid unimportant information.
3. Create parameters for collections by date ranges, custodians, subject matter, particular transactions, etc.

#### ABOUT THE AUTHORS

□ **Daniel V. Shapiro** is an Assistant United States Attorney in the Economic Crimes Unit and Computer Hacking and Intellectual Property Section of the United States Attorney's Office for the District of New Jersey. He also serves as the Criminal eDiscovery Coordinator for the District of New Jersey and as a member of EOUSA's Electronic Litigation Working Group.

□ **John Haried** is the Criminal eDiscovery Coordinator for the Executive Office for United States Attorneys (EOUSA) in the Department of Justice. He is an Assistant United States Attorney in the District of Colorado. He is a member of EOUSA's Electronic Litigation Working Group. He is an instructor for the Office of Legal Education at the National Advocacy Center on electronic management of case information and discovery-related topics. He previously wrote for the U.S. Attorneys Bulletin: USAO Options for Managing Small, Medium, and Large Cases (2016); The New Criminal ESI Discovery Protocol (2012); Flying Cars and Web Glasses: How the Digital Revolution is Changing Law Enforcement (2011).

Page Intentionally Left Blank

# Dismantling an Alien Smuggling Ring: Investigation and Prosecution Challenges for Federal Prosecutors

*Jason E. Corley*  
*Assistant United States Attorney*  
*Southern District of Texas*

*Eric Vincent Carroll*  
*Assistant United States Attorney*  
*Asset Forfeiture*  
*Southern District of Texas*

## I. Introduction

*“You can’t step in the same river twice.”—Heraclitus of Ephesus.*

Alien smuggling organizations (ASOs) operate for profit to transport and harbor individuals contrary to law. Yet, like all organizations both legal and illegal, each ASO has notable features that distinguish it from other ASOs. While all ASOs may have similar traits, these traits differ in extent and degree similar to distinct organisms of a common species. Investigations and prosecutions of different ASOs each present their own unique challenges. What works in the investigation and prosecution of one ASO might fail in the investigation and prosecution of another.

Nevertheless, three traits seem to be common among successful domestic alien smuggling organizations.<sup>1</sup> Long-lived and successful ASOs are (i) exclusive, (ii) engage in vertical integration, and (iii) resist horizontal integration. These three traits present the greatest challenges to law enforcement (LE) officials seeking to discover and investigate successful ASOs. Indeed, the presence of these traits in successful ASOs appear to be the result of natural selection in the alien smuggling community. In other words, if an ASO does not possess these traits, it does not survive because LE quickly discovers its existence, its participants, and the ASO’s modus operandi. While these traits may be beneficial to some ASOs in avoiding the prying eyes of LE, these same traits are deadly weaknesses to an ASO once LE identifies it. Prosecutors can and should guide LE to exploit these traits to both efficiently and thoroughly dismantle ASOs.

This article seeks to provide prosecutors insight into overcoming challenges presented when investigating and prosecuting alien smuggling rings. As such, this article begins with a discussion of three notable traits seemingly common among successful ASOs. Thereafter, the article focuses on practical and legal tools for overcoming those challenges.

---

<sup>1</sup> The focus of this article is on ASOs (or, as specified here, alien smuggling rings) principally operating within the U.S.

## II. The Alien Smuggling ‘Ring’

### A. Operate with Exclusivity

“*Speak ‘friend’ and enter.*”—Gandalf (THE FELLOWSHIP OF THE RING by J.R.R. Tolkien).

The characterization of an alien smuggling organization as a ‘ring’ may seem superficial, simplistic, and perhaps even artless. After all, the word ‘ring’ typically involves newlyweds at social gatherings, the MacGuffin of Tolkien novels, or the planet Saturn. It also commonly describes the boundary of a pugilist’s arena or the exhibition space of a circus. While the investigation and prosecution of an ASO—or alien smuggling ring—may often feel like a circus of evidence, this inquiry focuses on the characterization of the word ‘ring’ as “an *exclusive* combination of persons for a selfish and often corrupt purpose.”<sup>2</sup>

An understanding of the exclusive nature of their operation is the key to unlocking the evidence needed to prosecute many alien smuggling organizations along the southwestern border of the United States. Exclusivity separates an alien smuggling *ring* from a run of the mill and opportunistic ASO, the latter of which often involves interchangeable participants and a nebulous agreement or lack of agreement at all. Thankfully, exclusivity is also the Achilles’ heel of these operations once discovered.

Here, exclusivity refers to the close relationship between the participants of an alien smuggling conspiracy. For example, a conspiracy to harbor aliens that utilizes various stash-houses for short periods of time, works with various ‘coyotes’<sup>3</sup> in an opportunistic fashion, and employs temporary or rotating ‘polleros’<sup>4</sup> would not be described as exclusive. This type of ASO is inclusive. It will work with and employ many different individuals without loyalty to one another. The goal for an inclusive ASO is short-term profit. The term ‘ring’ does not aptly describe this type of organization because the participants do not form a closed group, or “exclusive combination.”

An alien smuggling ring, or exclusive ASO, is a tight-knit group of individuals, often family members or close friends, who utilize the same locations and participants for long periods of time with little growth or expansion. The goal for this type of operation is not short-term profit. Instead, the goal is long-term profit and low-risk methods of operation. Because these types of groups avoid interaction with individuals outside their circle of trust, they are difficult to discover and can remain concealed from LE for years or in some cases even decades.

Sometimes LE encounters exclusive ASOs, in some cases on multiple occasions, without learning the extent of the operation. This occurs because successful and long-lived alien smuggling rings often move few aliens or even a solitary alien on any single smuggling event, but may move hundreds or even thousands of aliens over a long enough timeline. Moreover, because law enforcement focuses on large seizures, and prosecution threshold guidelines typically demand multiple aliens for prosecution, an ASO may repeatedly interact with LE while only facing the cost of deportation for the seized alien.<sup>5</sup> From a prosecutorial standpoint, it is insufficient to charge one of these groups with the transportation of a single

---

<sup>2</sup> WEBSTER’S THIRD NEW INTERNATIONAL DICTIONARY 1958 (2002) (*Emphasis added*).

<sup>3</sup> The ‘coyote’ is the “arranger” who negotiates and works with an alien seeking transportation into the United States and/or harboring within the United States. The ‘coyote’ negotiates and arranges logistics with the alien’s family or sponsor like a travel agent.

<sup>4</sup> The ‘pollero’ is the guide who travels with the aliens by foot from a staging area in Mexico to a stash-house or “safe” location within the United States.

<sup>5</sup> For example, in a recent prosecution in the Southern District of Texas, an alien smuggling organization included a “capture fee” or “extra trip fee” as part of their overall charge for harboring and transporting aliens from the Rio Grande Valley to Houston. Included in the overall smuggling fee was the cost for two trips. If an alien was apprehended while using this organization, he/she was given one more smuggling attempt through the same organization at no additional charge because the alien already paid for that service prior to the first trip.

alien. Any attempt to prosecute an alien smuggling ring involving multiple participants over a long period of time necessitates a targeted and, in some cases, lengthy investigation.

Discovering these types of operations is not the only challenge as it relates to their exclusivity. Finding witnesses who are knowledgeable about the extent of the operation and who are willing to testify is an evidentiary challenge even after LE identifies this type of ASO. In any ASO where the participants are family members or close friends it can be difficult to acquire the assistance of an insider without tipping off the organization that LE is on their trail.

## **B. Engage in Vertical Integration**

*“The wise man puts all his eggs in one basket and watches the basket.”—Andrew Carnegie.*

Vertical integration “is the merging together of two businesses that are at different stages of production.”<sup>6</sup> In a well-known example, the Carnegie Steel company executed expansion by vertical integration in the late 19<sup>th</sup> century. Carnegie Steel owned steel mills and maintained control over a substantial amount of the steel production in the United States. Thereafter, Carnegie Steel expanded into their supply, the iron ore mines. Thus, Carnegie Steel exercised control over not only the production of steel, but also the supply of iron ore used to produce steel.

Less famous examples abound in the service industry. Here, the product sold to a consumer is a service, not a commodity like steel or iron ore. A fitting example is the vertical integration executed by hotels in most major cities in the United States. A hotel provides room and board (harboring). However, most large hotels in major U.S. cities also provide an airport shuttle (transporting). When hotels expand into the transportation market, or vertically integrate, they compete directly with taxi companies and other companies like Uber for consumers seeking transportation from the airport to the consumer’s destination. Unlike taxi companies and Uber, however, a hotel spreads the costs of transportation among customers who use and do not use the shuttle service.

Hotel companies have vertically integrated in other ways as well. Most large hotels in major U.S. cities have cleaning services for clothes (aiding and abetting a business meeting), restaurants and bars for entertainment (harboring), and in room pay-per-view entertainment (harboring). Each of these services directly competes with other niche service industries: movie theaters, nightclubs, and dry cleaners for example. Unlike the other businesses, however, the hotel offers these services under a single roof. This benefits both the customer and the hotel. The hotel keeps people on its premises spending money. The customer does not risk the time and expense of going elsewhere. Moreover, if an issue arises, the customer can deal with the same management.

Similar, if not identical, principals of vertical integration are present in the context of alien smuggling rings. ASOs and individual alien smugglers often have a niche, meaning they are either ‘smugglers’ (polleros), ‘harborers,’ ‘transporters,’ ‘document providers,’ or ‘arrangers’ (coyotes). They specialize.

An alien smuggling *ring*, however, expands—or vertically integrates—into different services while maintaining exclusivity. For example, three members of an alien smuggling ring might act as ‘harborers’ who use their own home as a stash-house. Two other members of the same ring might transport aliens while yet another member acts as a smuggler. Or they might all participate at random in each different service under the management of a leader/organizer.

This type of vertical integration provides the smuggled alien with a similar, if not identical, benefit to the customer of a large hotel. There is no need to go elsewhere for a service. The ‘arranger’

---

<sup>6</sup> *Vertical Integration*, THE ECONOMIST. (Mar. 30, 2009), <http://www.economist.com/node/13396061>.

‘coyote’<sup>7</sup> that the alien deals with in Mexico may have a working relationship with a particular alien smuggling ring. That smuggler can sell all of the services (smuggling, harboring, and transporting) as part of a single package with an up-front fee.<sup>8</sup> Thus, like the example of the hotel and the hotel shuttle competing with the taxi companies, the ASO engaged in vertical integration is in direct competition with other alien smugglers or transporters, even if their specialty is harboring aliens and providing false documents. So long as they are using the same smugglers in an ongoing fashion that establishes a formal agreement or informal understanding, the smugglers have joined the same conspiracy and are part of the same ASO forming a ‘ring.’<sup>9</sup>

Nevertheless, while successful alien smuggling rings operate with exclusivity, often times the alien smuggling ring is required to outsource a part of their operation. Sometimes this includes utilizing a legitimate business for their ends. For example, some ASOs specialize in harboring and providing documents for aliens, but also arrange travel by bus for their alien customer to the alien’s ultimate destination using those same false documents. The busing companies are unwittingly participating in the alien smuggling ring’s operation. Because the legitimate companies are unaware of their participation, exclusivity remains a feature of the ASO.

In an alien smuggling ring, trusted participants act exclusively for that particular ASO to fulfill all steps in the alien smuggling process. Thus, the participants of an exclusive and vertically integrated ASO often do not work with other alien smugglers and therefore reduce the risk of exposure to LE. In ASOs that are not vertically integrated, negotiations are often piecemeal through each step in the alien smuggling service chain. Because the vertically integrated and exclusive ASO is streamlined, efficient, and all-inclusive, it can be difficult to detect or disrupt with a single seizure.

### C. Resist Horizontal Integration

“*I like De Soto.*” (George)

“*De Soto? What did he do?*” (Jerry)

“*He discovered the Mississippi.*” (George)

“*Yeah, like they wouldn’t have found that anyway.*” (Jerry)—SEINFELD (NBC 1989-1998).

Horizontal integration occurs when there is merger between two firms in the same industry operating at the same stage of production.<sup>10</sup> A well-known example of horizontal integration occurred in 2015 when 3G Capital, an investment firm working with billionaire investor Warren Buffett of Berkshire Hathaway, purchased Kraft foods.<sup>11</sup> 3G Capital already owned Heinz, a competitor of Kraft in the condiment marketplace, and merged the two corporations to form the Kraft Heinz Company. 3G Capital was betting that the merger of these two companies competing for the same marketplace at the same stage of production would allow the combined companies to “cut costs and expand internationally.”<sup>12</sup> Regardless of the outcome for Buffett and 3G Capital, successful and long-lived ASOs seem to avoid this type of expansion.

---

<sup>7</sup> Again, in this context it is helpful to think of the ‘arranger’ or ‘coyote’ as a travel agent.

<sup>8</sup> In the case of highly sought after ASOs who have a good reputation, the fee for all services can exceed \$3,500.

<sup>9</sup> Indeed, in a recent prosecution in the Southern District of Texas, an alien smuggling ring utilized ‘passwords’ to ensure that aliens delivered to them by a guide were customers of the arranger’ or ‘coyote’ they trusted and worked with on an ongoing basis. This is representative of both exclusivity and vertical integration. The ASO in question only operated with those they trusted and those they had integrated into their operation.

<sup>10</sup> Tejvan Pettinger, *Horizontal Integration Definition*, ECONOMICS HELP (Nov. 28, 2012), <https://www.economicshelp.org/blog/glossary/horizontal-integration>.

<sup>11</sup> David Gelles, *Kraft and Heinz to Merge in Deal Backed by Buffett and 3G Capital*, THE NEW YORK TIMES (Mar. 25, 2015), [https://www.nytimes.com/2015/03/26/business/dealbook/kraft-and-heinz-to-merge.html?\\_r=0](https://www.nytimes.com/2015/03/26/business/dealbook/kraft-and-heinz-to-merge.html?_r=0).

<sup>12</sup> *Id.*

In the alien smuggling marketplace, horizontal integration involves adding more alien smugglers or guides (‘polleros’), more ‘harborers,’ and more transporters. An ASO that engages in horizontal integration expands in size in the same activity, and therefore increases their exposure to LE. For example, imagine two ASOs with eight participants each. Their specialty, or niche, is smuggling aliens across the Rio Grande River into south Texas. They merge to create one ASO with sixteen participants. After the merger, the participants (‘coyotes’ and ‘polleros’) share smuggling routes with one another that were previously exclusive to each individual ASO. The routes were exclusive either because the other was unaware of those routes or because one ASO did not have permission from higher powers to use those routes.<sup>13</sup> Once these two ASOs merge to become one ASO, and the routes are known to all involved, any arrest or seizure may have frustrating consequences if a participant provides LE with known routes.

Still, engaging in horizontal expansion may cause only logistical problems and not long-term failure for an ASO operating primarily in Mexico and that specializes in, or has a niche, smuggling aliens across the Rio Grande River, for example. In these types of operations, the goal is to move many aliens at once for short-term profit. As discussed above, this is partially due to cost. An alien smuggling ring that has vertically integrated can charge a costly up-front fee for an all-inclusive package of smuggling, harboring, and transporting. The specialist or niche ASO typically only charges for the single service provided.<sup>14</sup>

While horizontal expansion may be unbeneficial to specialty or niche ASOs, to the vertically integrated and exclusive alien smuggling rings, horizontal expansion can be disastrous. As discussed above, vertically integrated and exclusive ASOs provide services at each step of the supply chain, and they do this under one roof, so to speak. They may work exclusively with alien smugglers in an established and ongoing arrangement. They may harbor aliens at the same properties over long periods of time. And they may use the same transporters or methods of transportation consistently. They can charge higher fees while moving less aliens because they provide the all-inclusive package and do so efficiently with small numbers of participants. Put simply, their profit margins are higher.

If an exclusive and vertically integrated ASO (ring) expands horizontally, meaning that the ASO absorbs competitors into their tight-knit circle, that ASO risks exposure to the entire operation. Moreover, that risk is present at each step of the process or supply chain. Because this type of organization engages in smuggling, harboring, and transporting, one weak link in this chain can bring down the entire operation. Successful alien smuggling rings tend to survive by moving few aliens at any given time, but many aliens over the course of their operation, while remaining hidden from LE. Meanwhile, they seem to be instinctively aware of the risk of horizontal integration even if the participants are categorically unaware of the term.

Resisting horizontal integration is a survival trait for long-lived ASOs, particularly smuggling ‘rings’ as defined in this article. These ‘rings’ survive because of their relatively small size, because they are exclusive, and because of their ability to vertically integrate. Ordinary investigative techniques may ultimately lead to the discovery of most ASOs, especially those that horizontally integrate. An ASO that is exclusive, vertically integrated, and that resists horizontal integration presents a unique challenge to prosecutors and investigators. Nevertheless, there are ways to turn their strengths into weaknesses and ways to exploit those weaknesses to achieve an efficient and thorough dismantling of an alien smuggling ring.

---

<sup>13</sup> It is well known, at least in south Texas along the Rio Grande River, that alien smuggling is conducted with the permission of organized crime elements who expect to be compensated in one form or another through a ‘piso’ or extortion tax. Narcotics trafficking is typically reserved for certain parts of the river. Other parts of the river may be reserved for alien smuggling.

<sup>14</sup> Smugglers (‘polleros’), for example, typically charge anywhere from \$500 to \$1000 as a crossing fee. Thereafter, the alien or the alien’s sponsor (family member) must pay additional costs for harboring and transportation.

### III. The Investigation

#### A. Identifying the Alien Smuggling Ring

*“Alone we can do so little; together we can do so much.”—Helen Keller.*

Admittedly, the task of identifying an alien smuggling ring operating within the United States is primarily the responsibility of LE agencies and not federal prosecutors. More specifically, the task of identifying alien smuggling rings is the responsibility of the Department of Homeland Security.

Formed in 2002, The Department of Homeland Security (DHS) absorbed the responsibilities for maintaining the integrity of the borders of the United States. This included a transfer of the “Border Patrol program,” the investigations program (Immigration and Customs Enforcement or ICE), and the immigration “intelligence program” from the Commissioner of Immigration and Naturalization to DHS.<sup>15</sup> Following the transfer, DHS became responsible for “[c]arrying out the immigration enforcement functions vested by statute in, or performed by, the Commissioner of Immigration and Naturalization (or any officer, employee, or component of the Immigration and Naturalization Service).”<sup>16</sup> This includes:

- (i) “[e]stablishing and administering rules... governing the granting of visas or other forms of permission, including parole, to enter the United States to individuals who are not a citizen or an alien lawfully admitted for permanent residence in the United States;”<sup>17</sup>
- (ii) [e]stablishing national immigration enforcement policies and priorities;”<sup>18</sup> and,
- (iii) administering the customs laws of the United States.<sup>19</sup>

Agents working in Homeland Security Investigations (HSI), the investigative arm of U.S. Immigration and Customs Enforcement (ICE), are responsible for gathering intelligence that will lead to identifying and investigating alien smuggling rings. Nevertheless, federal prosecutors can provide important or, in some cases, critical guidance at the outset of any investigation.

In some cases, an investigation might begin from a ‘tip’ provided by an informant or concerned citizen. In other cases, assembled and analyzed data might lead investigators to begin targeting individuals suspected of engaging in alien smuggling and alien harboring. If the suspected ASO is functioning in a manner consistent with the three traits discussed earlier (exclusivity, vertical integration, and lack of horizontal integration), agents can quickly become frustrated by their inability to collect evidence without alerting the targets of the investigation. Often, a prosecutor’s most impactful role in the course of prosecuting an alien smuggling ring may be directing LE to gather evidence that may seem obvious in hindsight, but which no one bothers to seek at the outset.

#### B. Gathering Evidence—The Investigation

*“The world is full of obvious things which nobody by any chance ever observes.”—Sherlock Holmes (THE HOUND OF THE BASKERVILLES by Sir Arthur Conan Doyle).*

The swiftness of the prosecution and the thoroughness of the investigation are difficult factors to balance in an alien smuggling ring investigation. The case must be readily provable before it is prudent to present the matter to a Grand Jury for indictment. Yet, while the investigation is ongoing, the alien smuggling ring is actively transporting and harboring undocumented aliens within the United States. This

---

<sup>15</sup> Homeland Security Act of 2002, 6 U.S.C. § 251.

<sup>16</sup> § 202(3).

<sup>17</sup> § 202(4).

<sup>18</sup> § 202(5).

<sup>19</sup> § 202(6).

balancing act is present in the investigations of any ongoing criminal conspiracy, but it is particularly acute in the investigation of an alien smuggling ring because the amount of aliens a prosecutor can tie to that organization at sentencing largely determines the length of a conspirator's sentence.<sup>20</sup> There are quick and efficient ways to gather competent evidence without revealing the investigation to the ASO. Moreover, these investigative techniques attack the same traits that typically shield an ASO from detection: exclusivity, vertical integration, and a resistance to horizontal integration.

## **1. Learn the Parties—Attack Exclusivity**

As discussed above, alien smuggling rings operating in the United States often act exclusively. Because these organizations are often tight-knit—family and close friends—early efforts should focus on discovering all of the parties participating in the ongoing conspiracy once LE identifies an alien smuggler suspected of working with a larger ASO.

Moreover, LE will tangentially learn more about the method of operation, the properties involved, and the size of the operation simply by focusing on *who* is involved in the organization. Sometimes federal agents are excited to act, and they become distracted trying to build evidence on a single participant seeking a quick indictment. Prosecutors should resist this. It becomes far more difficult to gather evidence after indicting a party because the ASO learns of LE interest. Prosecutors should focus on discovering all of the parties involved first. There are methods of gathering this type of evidence without tipping off the ASO that an investigation is active.

### *'Trash Runs'*

Sometimes basic investigative techniques are the most fruitful. After identifying a suspected target, LE should consider a 'trash run' of the suspect's home. This may include multiple 'trash runs' over several weeks. A 'trash run' involves sifting through the suspect's garbage for receipts, ledgers, identifying documents, or anything else that may provide both identifying information of aliens previously smuggled and the past location information of conspirators. Co-conspirators likely visit the target's home, and receipts from cities outside the area will provide information regarding who is travelling frequently. Receipts and other documents may also shed light on the ASO's method of operation. For example, if there are dozens of receipts from Houston, Texas, found in a home in McAllen, Texas, it might be reasonable to assume the ASO is smuggling aliens through Houston. LE can coordinate with local waste management companies to achieve this subtly. To avoid detection by the target or targets of an investigation, waste management companies, if cooperative, can take garbage directly from a suspect's dumpster to the agents investigating the case.<sup>21</sup>

In some cases, there may be receipts or personal belongings of aliens previously apprehended by LE. Even if LE was unaware that the target ASO was moving a particular alien at the time of the alien's previous apprehension, LE can search DHS records for the alien's identifying information to discern a pattern in the movement of aliens utilizing the target's location.

Evidence preservation is paramount. This is more than intelligence gathering. Documents, ledgers, receipts, and any other identifying documents are useful evidence once a prosecution begins.

### *'Pole Cam'*

Another helpful tool when beginning an investigation of an alien smuggling ring is a hidden surveillance camera, generally called a 'pole cam.' After identifying at least one of the parties involved,

---

<sup>20</sup> U.S. SENTENCING GUIDELINES MANUAL § 2L1.1(B)(2) (U.S. SENTENCING COMM'N. 2016).

<sup>21</sup> This occurred in a recent investigation in the Southern District of Texas. A local waste management company picked up the garbage of a suspected target on multiple occasions and delivered the garbage to HSI agents. The HSI agents discovered bus receipts that led to surveillance footage of other targets buying tickets for undocumented aliens.

LE can install ‘pole cams’ on telephone poles, light poles, or any other public structure to observe who is going to and from a residence.

This accomplishes three objectives. First, the use of a ‘pole cam’ provides LE with physical identifiers of suspected co-conspirators coming to and from a property. Even if LE cannot identify parties entering a residence from facial recognition, it is not difficult to create a ruse to discover the identity of an unknown party. ‘Pole cams’ provide a live feed that LE can observe in real time. If an unknown party enters the residence, federal agents can request the assistance of local LE to discern the identity of the unknown party. When the party leaves the residence, a traffic violation is sufficient for an investigatory stop. LE can learn the identity of the party involved, and that individual will not suspect anything more than routine police interaction.

Second, the ‘pole cam’ stores the footage digitally. While the goal early in the investigation may be to identify parties involved, incontrovertible surveillance footage of a party at the scene is powerful evidence before a jury. Again, evidence preservation is paramount.

Third, if a prosecutor is lucky, a ‘pole cam’ may capture undocumented aliens entering and leaving the suspect’s residence. This may be difficult to observe in real time since the undocumented alien will likely be unfamiliar to LE, but preserved footage can be useful later if aliens are subsequently apprehended and cooperate.

#### *Other Surveillance Footage, Business Receipts, and ‘Tipsters’*

Many ASOs use false documents to take advantage of public and private transportation in the alien smuggling chain. Bus stations, private van companies, and taxis are often unwittingly (sometimes wittingly) used to move aliens from the border to the interior of the United States. If LE suspects an ASO of using one of these methods to transport aliens, LE can search a company’s receipts for suspects’ names. Thereafter, the timestamp on the receipt will often indicate when the target or multiple targets will appear on surveillance footage.

LE can use the receipts as a guide to collect footage of suspected targets’ interaction with other potential co-conspirators and undocumented aliens, providing deeper insight into all of the parties involved. The footage will also be a useful piece of evidence if properly preserved.

Further, law enforcement should recruit the assistance of employees or other innocent bystanders who frequent the location. For example, the employee of a busing company can notify LE any time one of the suspected targets purchases a ticket for another individual. With the help of an insider, LE will be able to gather more receipts and will be able to gather witnesses for prosecution.

## **2. Let the Aliens Come to Law Enforcement—Attack the Vertical Integration**

The method of operation for the ASO should be apparent once LE identifies all or most parties in an ASO. Because exclusivity is a common feature among ASOs, the parties identified typically engage directly in the acts of alien smuggling. While identifying the parties, LE will likely observe the method of operation. Is the ASO harboring aliens in residential properties? Do they have a stash house? Is the ASO transporting aliens to a stash-house? Is the ASO transporting aliens with personal vehicles? Is the ASO using private entities like busing companies? Is the ASO engaged in transporting, harboring, and document providing?

As discussed above, successful ASOs typically vertically integrate, meaning they provide multiple services to an alien. As such, an alien smuggling ring will likely be engaged in both harboring and transporting undocumented aliens. Some ASOs may also be involved in providing false documents. LE should not rush to seize harbored or transported aliens unless there is an imminent danger, which includes both the risk to aliens who might be the victims of violence or extortion and/or the risk to the general public if the transported and harbored aliens are suspected dangerous individuals. Excluding those

scenarios, LE should allow the aliens to come to them. This involves cooperation with Customs and Border Protection, Border Patrol, and local LE to maintain the illusion that the ASO is not under investigation.

### Gathering Witnesses

Once LE discovers the target ASOs method of operation, LE should coordinate efforts with Border Patrol, U.S. Customs and Border Protection (CBP), or local LE, and allow the aliens to come to federal authorities, who will be waiting for them when they arrive. For example, if an ASO is utilizing false documents to transport aliens on a bus from the border to the interior of the United States, LE should request the support of CBP officers at the border checkpoint where the bus is travelling. If the ASO used personal vehicles to transport aliens, a pretext stop that leads to a seizure of aliens is an effective method of gathering witnesses. At this time, barring extraordinary circumstances, the alien smuggler should not be arrested. An exception to this rule may include alien smugglers operating in the brush due to the inherent danger presented to all parties involved, including LE.

Thereafter, the agents investigating the ASO can meet with the smuggled aliens to accomplish three primary objectives. First, the aliens can provide first-hand knowledge regarding the stash-house location and information regarding where they were smuggled. Moreover, because law enforcement has already identified many, if not all, of the parties involved, law enforcement can ask the aliens to identify those parties in photo lineups. In many cases, the aliens will also provide detailed information on which participants engage in certain activities, how the aliens were treated, and what other aliens they may have interacted with along the way. In some cases, the aliens are willing to cooperate in exchange for “conditional parole” into the United States pursuant to Section 236 of the Immigration and Nationality Act.

Section 236 of the Immigration and Nationality Act accomplishes the second objective. Section 236 allows for the “conditional parole” of an apprehended, undocumented alien.<sup>22</sup> United States Immigration and Customs Enforcement (ICE) can release an apprehended alien into the United States and require that alien to report regularly to an ICE agent.<sup>23</sup> This provision can be a useful tool in gathering witnesses as well as other evidence. Rather than indicting the ASO at the time of the seizure and designating the aliens as material witnesses, LE can gather many more witnesses by allowing the “conditional parole” of aliens who do not pose a danger to the American public and who are willing to testify at a later date. In many jurisdictions, this can assist prosecutors in avoiding the need for depositions. Moreover, this method avoids the strict deadlines imposed by speedy trial requirements if the smuggler is arrested at that time.

Finally, aliens often travel with cellular phones. Pursuant to a border search, LE can dump the contents of an apprehended alien’s phone to gather direct evidence of the smuggling activity.<sup>24</sup> Often the smuggled aliens have pictures in their phones. Sometimes the images depicted will prove useful as evidence at trial.<sup>25</sup> But even if the image depicted appears immaterial, metadata contained within the digital file may contain location information that may serve as useful evidence at trial or useful intelligence for further investigation. Thus, even an uncooperative alien may have evidence on their

---

<sup>22</sup> 8 U.S.C. § 1226(a)(2)(B).

<sup>23</sup> ICE Form I-220A (8/15) is the form provided for ICE agents to utilize the “conditional parole” provision of 8 U.S.C. § 1226(a)(2)(B).

<sup>24</sup> Border search authority is expansive despite recent appellate decisions. *See* *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013). Here, however, suppression is not a concern. Future defendants do not have standing to challenge the search of aliens’ phones.

<sup>25</sup> For example, in a recent prosecution in the Southern District of Texas, a smuggled alien had the image of the alien smuggler’s dog. This image contained metadata providing the location that the image was taken—inside the defendant’s home.

person. This may also include physical evidence such as receipts or other items provided by an alien smuggler.

If LE manages to achieve this type of seizure on few or many occasions, the prosecution may have gathered testimonial evidence, digital evidence, and physical evidence without alerting the ASO that an investigation into the ASOs activity is underway.

#### *Continue Surveillance and ‘Trash Runs’*

After LE apprehends aliens in the manner described above, LE should continue to utilize ‘trash runs,’ ‘pole cams,’ and other surveillance to corroborate the testimony of the aliens allowed conditional parole into the United States. For example, the same alien apprehended at a checkpoint travelling on a bus may have thrown something out at the stash-house that is now in the garbage. ‘Pole cam’ footage may have recorded a paroled alien entering and leaving one of the ASO’s stash-houses. Likewise, there are likely recordings of the alien smugglers and the alien on the bus station surveillance if the ASO is using other forms of transportation. The same methods previously used to identify the parties are effective at corroborating information provided by aliens who will testify as witnesses in a potential future trial.

### **3. The Seizure—We are Big, They are Small**

As discussed above, successful ASOs resist horizontal integration. This means that most alien smuggling rings are relatively small. The conspiracy may only involve a dozen or so participants—sometimes even fewer. If residential properties are used as stash-houses, they may be few as well. While a resistance to horizontal integration was beneficial to the ASO in avoiding law enforcement, the relatively small size of the operation presents an extraordinary opportunity when the investigation reaches the indictment stage.

#### *Strike All Parties at Once*

When the prosecution is readily provable, meaning there are sufficient witnesses and there is sufficient physical evidence to prove the case beyond a reasonable doubt to a petit jury, a prosecutor can work with LE to obtain search warrants for all addresses involved, including residential properties and/or stash-houses. The search warrant should include cell phones, computers, and other digital storage devices that may contain communications between co-conspirators, ledgers and records of smuggled aliens, and GPS data records from past travel. LE should execute the search warrants on the same date the Grand Jury indicts the parties for alien smuggling and arrest warrants are issued pursuant to the indictment.

LE should search all the residence stash-houses simultaneously. Likewise, LE should arrest the indicted co-conspirators simultaneously. This may seem like common sense, but LE may be resistant to the idea. This type of operation might involve hundreds of agents and present a logistical hurdle. Nevertheless, LE may discover an abundance of evidence and gather more alien witnesses because the ASO will not have time to destroy and hide evidence or move aliens to a different location.

#### *Put the Parties Together*

After LE executes the search warrants and arrests the conspirators, the act of putting all of the ASO’s co-conspirators together in one place is a useful investigative tool. This involves the use of a large detainment cell or the use of a large van. LE should place a hidden camera inside the cell or van and allow the parties to interact freely. This investigative trick turns the ASO’s exclusive nature into a trait that benefits the investigation rather than the conspirators.

Because alien smuggling rings are exclusive (tight-knit; often family or close friends), placing all of the ASO’s conspirators into one place while a camera records their interactions will likely generate powerful evidence. First, if the investigation has maintained the veil of secrecy, this will be the first time the ASO’s conspirators learn that they are the target of an investigation. The shock of this revelation may be enough to cause outbursts of blame towards one another or other useful *res gestae* statements. Second,

in any organization, there is a leader/organizer. That individual will likely attempt to concoct a strategy to deal with LE going forward. Third, if LE failed to identify a party involved in the ASO, the detained conspirators may identify that individual in a conversation due to that individual's absence.<sup>26</sup>

Before LE interviews the conspirators, the case agent should review the footage. For an alien smuggler, the realization that they have already been recorded discussing details of the offense may be enough to change their temperament during a custodial interview.

### **C. Selling the Evidence—The Prosecution**

*“The supreme art of war is to subdue the enemy without fighting.”—Sun Tzu, THE ART OF WAR.*

The greatest challenge in the prosecution of an alien smuggling ring is organization. If LE effectively gathered both evidence and witnesses, and if the investigation led to the indictment of perhaps a dozen or more defendants, the most daunting and intimidating challenge for any prosecutor is not finding evidence; the challenge is organizing too much of it. Like any prosecution, this will involve two forms of evidence: testimonial and physical. Generally, a prosecutor should begin by organizing the testimonial evidence first before organizing the corroborating physical evidence.

#### **1. Organize the Testimonial Evidence from the Smuggled Alien's Perspective**

Testimonial evidence in the prosecution of an alien smuggling ring includes written statements by LE in the form of reports (ROIs). The reports generated by LE will include the written recollections and actions of the agents investigating the case, as well as the summarized statements of other witnesses discovered during the investigation.

Other witnesses will include any aliens granted “conditional parole” under Section 236 of the Immigration and Nationality Act. It can be challenging to keep track of which aliens interacted with particular defendants during the course of the ASO's ongoing activities. Likewise, it can be an even greater challenge organizing the statements made by these witnesses into a coherent order that coincides with the chronological order of the investigation. It can be helpful to create a timeline based on the movement of the aliens rather than the overt acts of the conspirators.

As previously discussed, an alien smuggling ring provides a service in a vertically integrated fashion. A simple and helpful way to organize testimonial evidence can capitalize on the vertical integration of the ASO by organizing the testimonial evidence in a similar fashion.

Thus, a prosecutor should generally begin by creating a timeline starting with the first alien witness, meaning an alien granted conditional parole, with the start date being the date the alien was smuggled from a foreign country (typically Mexico) into the United States. Thereafter, a prosecutor can fill in significant dates, including when the ASO smuggled the alien to a stash-house, if the alien was moved to a different stash-house, when the alien was provided false documents, when the ASO attempted to move the alien north into the interior of the United States, and the date the alien was apprehended. Along the timeline, it is helpful to note whom the alien witness interacted with in the conspiracy. Thereafter, a prosecutor can build on the same timeline with subsequent alien witnesses in chronological order.

---

<sup>26</sup> Indeed, in a recent investigation in the Southern District of Texas where this investigative method was employed, the co-conspirators of the ASO involved provided LE with all three: (1) the co-conspirators blamed one another and made repeated inculpatory statements; (2) the leader organizer directed certain individuals to take the blame and demanded that she be exculpated by the others; and (3) the co-conspirators identified an absent party.

## 2. Organize the Physical Evidence from Law Enforcement's Perspective

After a prosecutor has organized the testimonial evidence into a timeline from the aliens' perspective, a clear picture should emerge detailing the extent of the ASO's activities. Thereafter, the physical evidence serves to corroborate the live testimony of the alien witnesses. A prosecutor can add to the same timeline created for the alien witnesses and plug in physical evidence at the dates law enforcement discovered the physical evidence.

For example, if an alien was apprehended at an immigration checkpoint and metadata containing GPS coordinates was discovered in an image on the alien's phone, a prosecutor should plug the discovery of that information into the timeline from the date law enforcement made the discovery. This serves two functions, both of which aim for trial strategy. First, it organizes trial testimony. A federal agent cannot testify that the alien was present at the address in question. Only the alien witness can testify to that fact with certainty. Instead, a federal agent can testify that the metadata found in an image on the alien's phone indicates the alien was present at the address. This corroborates the alien witness's testimony, but does not put the agent in the position of testifying to hearsay or to something he or she does not know. Second, in a typical jury trial the case agent will testify after the alien witnesses. By holding back the physical evidence and allowing the alien witnesses to speak from memory, the prosecution puts the defense in an awkward position. If the defense attacks the alien witnesses too vigorously, the revelation that physical evidence corroborates the earlier testimony will not sit well with a jury.

## 3. Create a 'Trial File'

Once a prosecutor has created a coherent and trial-ready timeline, the goal is to sell the evidence to the defense. Here, there are two key points. The first goal is to organize the evidence in a manner that is easy for defense counsel to digest. This does *not* mean organizing *all* of the evidence into a presentable format. That is burdensome not just for the prosecution team, but also for the defense. Create two different files of evidence, both of which are available for discovery for the defense lawyer. The first file is the 'master file.' This file will more likely take the form of a large cardboard box (or two or four . . .) and will contain all of the evidence gathered during the investigation. This will typically be organized in the order the ROIs were generated and the evidence was gathered. Should the defense choose to immerse themselves in the depths of an alien smuggling ring investigation, that option should certainly be made available to them.

However, a prosecutor can also prepare a second file. The second file may be called the 'trial file,' though it might as well be called the 'plead guilty file.' It can be helpful to organize this file with duplicates of the strongest evidence contained in the 'master file' in an order consistent with the previously created timeline, meaning from the smuggled aliens' perspective rather than the chronology of the investigation. The goal is to convincingly and plainly demonstrate the competence of the investigation and the strength of the government's case. It is helpful to include only the strongest evidence that clearly demonstrates the guilt of the defendants rather than every piece of inculpatory information. An effective 'trial file' is easy to read, easy to grasp, and easy for the defense lawyer to thereafter discuss with his or her client. Defense lawyers are not only looking for weaknesses in the government's case, but also for easy-to-explain evidence that they can relay to their client to fulfill their duties before a guilty plea. A simple and easy-to-grasp 'trial file' compels early pleas of guilty.

Moreover, by organizing the 'trial file,' the prosecution can map out the theme and theory of the prosecution long before any talk of trial begins. A prosecutor can draw from the 'master file' to fill in gaps or to strengthen the case later if needed. But from the outset, if a prosecutor has a 'trial file' and readily shares this file with the defense, the defense will be subdued by the prosecution's preparation and will less vigorously scrutinize the 'master file.'

The second key point is to preserve the integrity of the prosecution. If there is exculpatory or mitigating evidence, it is helpful to *include it* in the trial file. Showing this evidence directly to defense

counsel along with all of the other competent and powerful evidence the prosecution possesses achieves two objectives. First, this act goes above and beyond the prosecution’s discovery obligations pursuant to the Federal Rules<sup>27</sup> and *Brady*.<sup>28</sup> Discovery obligations are met simply by making the ‘master file’ organized and available. Nevertheless, providing the evidence directly not only demonstrates integrity, it shows confidence in the strength of the case. Second, the conspirators of the ASO (the clients of the defense attorneys) are aware of who is more culpable and who is less culpable in an alien smuggling ring. Again, these are tight-knit groups acting exclusively with one another. They already know about any exculpatory or mitigating evidence in a prosecutor’s possession. They already know which participant is most at fault and who the leader/organizer is. When a prosecutor provides the information readily to defense counsel, along with the other compelling evidence that overcomes and overwhelms the exculpatory and mitigating evidence, a prosecutor preemptively provides defense counsel with the reasons his or her client should plead guilty despite the client’s apparent lesser role.

## D. The Indictment

*“Our life is frittered away by detail. Simplify, simplify, simplify!”* —Henry David Thoreau.

Federal law provides multiple ways to indict and prosecute individuals involved in alien smuggling within the United States. Indeed, a prosecutor preparing to indict an alien smuggling ring might be able to construct a dozen different types of charges for the same conduct. Recent memoranda dictate “a core principal that prosecutors should charge and pursue the most serious, readily provable offense.”<sup>29</sup>

Unless the smuggling of an alien resulted in serious bodily injury,<sup>30</sup> placed in jeopardy the life of any person,<sup>31</sup> or resulted in the death of any person,<sup>32</sup> the most serious and readily provable charge that is typically available to prosecutors charging an alien smuggling ring is the conspiracy provision under Title 8, United States Code, Section 1324(a)(1)(A)(v)(I). This provision provides for a maximum sentence of ten years<sup>33</sup> and removes any need for a Title 18 U.S.C. § 371<sup>34</sup> conspiracy charge.

An added benefit of the conspiracy provision of Section 1324 is that it also removes the necessity of an alien witness to establish alienage. Indeed, appellate courts have yet to establish conclusively what elements are required to sustain a conviction under this charge. Some courts have even suggested that a 1324 conspiracy charge does “not require proof of an overt act.”<sup>35</sup> Although the statute may not require either proof of an overt act or an alien witness to establish alienage, best practice speaks otherwise.

A simple and effective indictment will track the investigative timeline discussed above, which was based on the overt acts of the alien smuggling ring from the perspective of the aliens smuggled. An indictment sought on a vertically integrated alien smuggling ring for conspiracy can allege all four

---

<sup>27</sup> FED. R. CRIM. P. 16.

<sup>28</sup> *Brady v. Maryland*, 373 U.S. 83 (1963).

<sup>29</sup> Memorandum for all Federal Prosecutors, Office of the Attorney General, *Dep’t. Charging & Sentencing Policy* (May 10, 2017).

<sup>30</sup> 8 U.S.C. § 1324(a)(1)(B)(iii).

<sup>31</sup> § 1324(a)(1)(B)(iii).

<sup>32</sup> § 1324(a)(1)(B)(iv).

<sup>33</sup> § 1324(a)(1)(B)(i).

<sup>34</sup> 18 U.S.C. § 371.

<sup>35</sup> “Appellants concede that the Supreme Court has not ruled on whether 8 U.S.C. § 1324 requires proof of an overt act, and this circuit has declined to address the issue. Further, the statute is silent on whether an overt act is required, and the Supreme Court has held that similarly silent criminal code sections do not require proof of an overt act.” *United States v. DeLeon*, 484 F. App’x 920, 927 (5th Cir. 2012) (*unpublished*); *citing* *Wilkinson v. Austin*, 545 U.S. 209, 214 (2005); *United States v. Shabani*, 513 U.S. 10, 13-14 (1994).

substantive ‘manner and means’ provided for in Section 1324:

- (1) *1324(a)(1)(A)(i)* – bringing or attempting to bring an alien to the United States at a place other than a designated port of entry;
- (2) *1324(a)(1)(A)(ii)* – transporting or moving or attempting to transport and move an alien within the United States;
- (3) *1324(a)(1)(A)(iii)* – concealing, harboring, or shielding from detection an alien that has come to or entered the United States; and,
- (4) *1324(a)(1)(A)(iv)* – encouraging or inducing an alien to come to, enter, or remain in the United States.

Thus, the aforementioned vertical integration of the alien smuggling ring can be used as a tool for prosecution in a single conspiracy count. An alien smuggling ring can be charged in a single count with conspiring to bring or attempt to bring aliens into the United States; transporting or attempting to transport aliens within the United States; concealing, harboring, and shielding from detection aliens within the United States; and encouraging and inducing aliens to enter or remain within the United States.

Thereafter, best practice may dictate alleging substantive counts for each alien witness for “bringing,” “transporting,” “harboring,” and “encouraging,” depending on the evidence available. It might be prudent to allege only the conspirators that interacted with each individual alien for each substantive count alleged.

This process flows directly from the nature of the alien smuggling ring—its vertical integration—and also draws upon the timeline created during the investigation as well as the ‘trial file’ created to negotiate with defense counsel. In the case of prosecuting alien smuggling rings, a simple and plain reading indictment that avoids the minutiae of a long investigation is a prosecutor’s ally.

## E. Forfeiture

*“In the house of the righteous is much treasure: but in the revenues of the wicked is trouble.”*—Proverbs 15:6 (King James).

A key tool for the effective dismantling of alien smuggling rings is asset forfeiture. The primary purpose of the asset forfeiture program “is to employ the federal asset forfeiture authorities in a manner that enhances public safety and security. This is accomplished by removing the proceeds of crime and other assets relied upon by criminals and their associates to perpetuate criminal activity against our society.”<sup>36</sup>

Asset forfeiture can be used to strengthen the criminal case against alien smugglers, weaken the criminal enterprise behind alien smuggling, and return illegal proceeds to the victims of the crime. Criminal AUSA’s should consult with and involve their office’s Asset Forfeiture Section attorneys as early as possible in alien smuggling case investigations for several reasons. First, depending on the nature of the asset targeted for forfeiture, certain consultations must take place, or approvals obtained, before some assets can be restrained, seized, or forfeited. For example, it is not uncommon for alien smuggling investigations to involve ongoing businesses, particularly restaurants, that are used to facilitate the alien smuggling and harboring. When the restraint, seizure, or forfeiture of an ongoing business could create a deficit to the Assets Forfeiture Fund, then the Justice Management Division, Asset Forfeiture Management Staff (JMD) must give approval, in coordination with the Money Laundering and Asset Recovery Section (MLARS).<sup>37</sup> Another example involves contaminated real property—before

<sup>36</sup> ASSET FORFEITURE POLICY MANUAL (2016), ch. 1, § I.A.

<sup>37</sup> ASSET FORFEITURE POLICY MANUAL (2016), ch. 1, § I.D.4; ch. 10, § IV.

contaminated real property can be forfeited, the investigating agency, the United States Marshals Service (USMS), MLARS, and the JMD must be consulted.<sup>38</sup> Second, Asset Forfeiture attorneys work with the investigative agency's asset removal group to obtain necessary documents (e.g., net-equity analysis, title commitment reports, ownership records) to evaluate the forfeiture. Third, sufficient time is needed to draft forfeiture notices for indictments, draft seizure warrants before searches or arrests, and prepare notices of lis pendens for filing in the property records.

Authority for forfeiting assets in criminal alien smuggling and harboring cases is found in Title 18, U.S.C., Section 982(a)(6); and in Title 8, U.S.C., Section 1324(b) in conjunction with Title 28, U.S.C., Section 2461. For example, under § 982(a)(6), the following property is subject to criminal forfeiture in alien smuggling/harboring cases:

- Any conveyance, including any vessel, vehicle, or aircraft used in the commission of the offense of which the person is convicted;
- Any property real or personal that constitutes, or is derived from or is traceable to the proceeds obtained directly or indirectly from the commission of the offense of which the person is convicted; and
- Any property real or personal that is used to facilitate, or is intended to be used to facilitate, the commission of the offense of which the person is convicted.

Title 18, U.S.C., Section 982(a)(6)(A)(i) and (ii). Common properties subject to forfeiture in alien smuggling and harboring cases include cash proceeds, real property,<sup>39</sup> and vehicles.<sup>40</sup>

Bringing in and harboring aliens in certain circumstances also constitutes “specified unlawful activity” for purposes of money laundering.<sup>41</sup> In those situations, the broad “involved in” language of the money laundering forfeiture provision of Title 18, U.S.C., Section 982(a)(1) applies,<sup>42</sup> thereby expanding the scope of the property subject to forfeiture.

## F. Conclusion

Successful alien smuggling rings possess three traits that shield them from law enforcement, including: exclusivity, vertical integration, and resistance to horizontal integration. A prosecutor and the investigative team should embrace these traits and adapt to them in the investigation and prosecution of alien smuggling rings. An investigation that focuses on these traits will move swiftly and competently. A prosecutor that embraces these traits to organize the theory, theme, and evidence of an alien smuggling ring prosecution will enjoy relatively painless success without the need for a jury. Forfeiture of the alien

---

<sup>38</sup> ASSET FORFEITURE POLICY MANUAL (2016), ch. 13, § I.A.

<sup>39</sup> *United States v. Cantu*, 542 F. App'x 380, 381 (5th Cir. 2013) (real property used to conceal aliens from law enforcement, and harbor them waiting for transport to another location, is forfeitable as facilitating property under § 982(a)(6)); *United States v. George*, 779 F.3d 113 (2d Cir. 2015) (affirming forfeiture of residence where illegal alien was harbored and employed as a servant at less than minimum wage for 5 years); and *United States v. Sabhnani*, 599 F.3d 215, 262 (2d Cir. 2010) (residence where aliens are harbored and subjected to involuntary servitude is forfeitable as facilitating property under both § 1594 and § 982(a)(6)).

<sup>40</sup> *United States v. Munoz-Escalante*, No. CR 13-50154-01-KES, 2014 WL 2574535, at 4 (D.S.D. June 9, 2014) (construction vehicle being operated by illegal alien subject to forfeiture as vehicle used in commission of a harboring offense under § 1324(a)).

<sup>41</sup> 18 U.S.C. § 1961(1)(F) (“racketeering activity” means . . . (F) any act which is indictable under the Immigration and Nationality Act . . . if the act indictable . . . was committed for the purpose of financial gain.”).

<sup>42</sup> *United States v. Schlesinger*, 396 F. Supp. 2d 267, 271-72 (E.D.N.Y. 2005) (“The term ‘involved in’ has consistently been interpreted broadly by courts to include any property involved in, used to commit, or used to facilitate the money laundering offense.”), and cases cited therein.

smuggling ring's assets completes the dismantling of an organization that may have been acting with impunity for years. A prosecutor may not be able to "step in the same river twice," but he or she can certainly use the same boat to cross whatever river he or she faces.

#### **ABOUT THE AUTHORS**

□ **Jason E. Corley** is an Assistant United States Attorney for the Southern District of Texas, Brownsville Division. Mr. Corley has served as an Assistant United States Attorney since 2014. Mr. Corley works in the Criminal Division and is a member of the RGV Child Exploitation Task Force.

□ **Eric Vincent Carroll** is an Assistant United States Attorney for the Southern District of Texas, Houston Division. Mr. Carroll has served as an Assistant United States Attorney since 2005. Mr. Carroll works in the Asset Forfeiture Division and is an asset forfeiture liaison with the Houston Strike Force as well as the Southern District of Texas-Houston Organized Crime Drug Enforcement Task Force.

# In Search of Shadows: Investigating and Prosecuting Crime on the “Dark Web”

*Keith Becker*  
*Deputy Chief*  
*Child Exploitation and Obscenity Section*

*Ben Fitzpatrick*  
*Senior Counsel*  
*Computer Crime and Intellectual Property Section*

Technologically sophisticated offenders deploy a multitude of strategies to perpetrate online-facilitated crimes without getting caught. This article will discuss common technological and legal challenges presented when investigating and prosecuting criminals who use the so-called “Dark Web.”

## I. What is the “Dark Web”

Consider the internet in three related parts, commonly depicted as an iceberg with some part of the structure above the water’s surface and a larger part below: *first*, above the water line is the “Open Internet,” that is, publicly-accessible web pages that can be “crawled” or “indexed” by search engines such as Google so that internet users may search for content that is contained on those web pages; *second*, below the water line and commonly reported to be the largest portion is the “Deep Web,” that is, web pages whose contents are not crawled or indexed by standard search engines, generally because they are within internal corporate, government, or academic computer networks or behind subscription or pay walls; and *third*, further below is the “Dark Web,” that is, a sub-part of the “Deep Web” consisting of computer networks that require specific software or software configurations to access.

### A. What Does the Dark Web Allow Users to Do

The primary feature of a Dark Web computer network is that it allows users to communicate over the internet anonymously. Dark Web networks offer all of the same kinds of communication platforms as the open internet—websites, chat, file sharing, etc.—with the added benefit of robust anonymity. The most popular Dark Web network—and unsurprisingly, one that factors into numerous law enforcement investigations—is the Tor network.

## II. What is the Tor Network

The Tor network is designed to provide anonymity to users by encrypting and then routing online communications through a network of relay computers run by volunteers all around the world. This prevents the end recipients of communications from learning a user’s internet protocol address (IP address), which could otherwise be used to identify a user. Originally created by the United States Naval Research Laboratory to protect government communications, it is currently run and maintained by the nonprofit Tor Project. To access the Tor network, a user must install Tor software, which is most easily accomplished by downloading the free “Tor browser,” a version of the “Mozilla Firefox” web browser

that is pre-configured to communicate via the Tor network. Information documenting what Tor is and how it works is provided on the publicly accessible Tor website at [www.torproject.org](http://www.torproject.org).

## A. How Does Tor Provide Anonymity

Tor software provides for user anonymity in two primary ways: *first*, by allowing Tor users to access ordinary “Open Internet” websites without revealing their IP addresses to the website; and *second*, by allowing users to operate (and access) Dark Web websites, called “hidden services,” whose actual server location is obscured.

Let’s first examine Tor’s use for anonymous internet communications. Ordinarily, when an individual accesses a website (such as [www.justice.gov](http://www.justice.gov)), that user’s IP address information is transmitted to the website’s computer server (a “web server”) and recorded in the server’s logs. Using legal process, investigators can obtain those logs and then compel an internet service provider to disclose basic subscriber information about the customer to which a pertinent IP address was assigned—information that is critical to trace internet communications to specific devices and individuals.

When a person uses Tor to access the same ordinary internet website, however, communications between the Tor user’s computer and the web server are routed through a series of intermediary computers. As a result, only the IP address of the last computer through which the Tor user’s communications were routed (which is known as the “exit node”) is revealed to, and recorded by, the web server. Thus, any IP address logs on that web server would not contain the actual IP address of a Tor user’s computer. By masking a Tor user’s true IP address, Tor effectively conceals the actual location of Tor users’ computers. A criminal suspect’s use of Tor accordingly makes it extremely difficult, if not impossible, for law enforcement agents who are investigating online crime to determine a Tor user’s physical location.

In addition to providing a means for users to access the internet without revealing their true IP addresses, Tor also makes it possible for users to operate and use websites—which Tor calls “hidden services”—on the Dark Web. Like ordinary internet websites, hidden services are hosted on computer servers that communicate through IP addresses. However, hidden services bear unique technical features that conceal the computer server’s location.

In the case of an ordinary internet website (such as [www.justice.gov](http://www.justice.gov)), a publicly available query can be performed, via a Domain Name System (DNS) listing, to determine the IP address of the computer server that hosts the website. Further publicly available queries may be run regarding that IP address to determine the owner and location of the computer server. Legal process may then be served on the owner or operator of that computer server in order to lawfully obtain information about, or the contents of, that computer server.

As distinguished from an ordinary internet web address (such as [www.justice.gov](http://www.justice.gov)), a Tor-based web address is comprised of a series of sixteen algorithm-generated characters, such as “asdlk8fs9df1ku7f,” followed by the suffix “.onion.” Unlike ordinary internet websites, there is no publicly available query that may be performed via a DNS listing to determine the IP address of the computer server that hosts a Tor hidden service. Moreover, communications between users’ computers and a Tor hidden service web server are routed—as with all Tor communications—through a series of intermediary computers. Accordingly, neither law enforcement nor hidden service users can determine the true IP address—and therefore the location—of the computer server that hosts a hidden service through public lookups or ordinary investigative means. Such a website can effectively be hosted anywhere in the world without accountability to any government or law.

### **III. How Do Criminals Exploit the Dark Web**

Unsurprisingly, criminals take full advantage of the anonymity afforded by Tor and other anonymous services to engage in a wide variety of illegal activity, for example, to hide their identity while perpetrating crimes such as swatting (falsified calls to emergency services made to generate a police response), cyberstalking (use of the internet to harass a victim), or sextortion (an attempt to extort sexually explicit images from a victim, usually via threat to disseminate other such images), and to access internet e-mail, social networking, or other online accounts without leaving an identifiable trail.

#### **A. What Technologies Do Offenders Use to Maintain Anonymity**

Anonymous networks like Tor make up only one type of technologically sophisticated, online tool that criminals can deploy in order to avoid detection by law enforcement. Virtual Private Networks (“VPN”), proxy servers, anonymous e-mail providers, and other web services that neither retain nor provide any identifying information in response to lawful legal process can make it virtually impossible for law enforcement to track down the identity and location of criminal suspects. End-to-end encrypted communication channels provide another mechanism for online criminals to ensure that, even with appropriate court-authorization, law enforcement agencies cannot surveil communications regarding ongoing criminal schemes. Furthermore, the ever-more widespread use of virtual currencies and secondary services that help launder illicit proceeds create significant challenges to tracing illicit payments. Foremost among them is the difficulty in obtaining records from the virtual currency operators that could help investigators conclusively identify the participants in a criminal transaction, as well as the difficulty in tracing transactions made with virtual currencies.

Compounding the investigative problems inherent in these anonymizing technologies is the global and borderless nature of all internet-facilitated crime—which means not only that evidence may be located on computer servers anywhere in the world, but also that criminal actors may engage in a so-called race to the bottom—seeking out web hosting services or other online platforms in jurisdictions perceived to be beyond law enforcement’s reach. A significant challenge that this causes is that to obtain evidence located abroad, United States law enforcement may have to rely on the criminal laws of other countries and an often-cumbersome mutual legal assistance treaty (MLAT) process, which too often does not operate at the speed needed to effectively investigate cybercrime.

#### **B. What Unique Problem is Posed by Tor Hidden Services**

Fully anonymous platforms such as Tor hidden services, however, pose a unique and significant threat to public safety. In that environment, offenders set up websites exclusively dedicated to criminal aims that operate openly and notoriously. Law enforcement agents can access the sites and document the content and criminal activity taking place, but are unable to utilize the sort of investigative steps—a combination of publicly available queries and legal process—that would ordinarily allow them to timely determine where the crimes are occurring and who is perpetrating them. The fact that law enforcement can generally identify evidence and perpetrators when crimes occur via ordinary internet websites deters offenders from engaging in open and notorious criminal activity via the internet. Absent that crucial deterrence effect, criminal hidden services stabilize and grow.

This phenomenon is perhaps most evident in the persistent problem of criminal child exploitation communities that operate via Tor hidden services, where like-minded child sex offenders gather to promote and normalize the sexual abuse of children, educate each other about how to perpetrate child sex abuse without getting caught, and share images and videos depicting the sexual abuse and exploitation of children as young as infants and toddlers. Such communities are disturbingly commonplace and frequently involve tens of thousands of members. In addition, so-called Dark Markets—where offenders may buy, sell and trade illicit goods such as narcotics, firearms, credit card numbers, hacking tools and ill-gotten, personally identifying information in an environment that protects the anonymity of criminal

sellers and purchasers—also abound. In the midst of an opioid crisis occurring in the United States, the open availability of Dark Markets, where illicit narcotics are freely available, poses a significant public health threat.

Anonymizing technology like Tor software not only provides criminals with a platform on which to conduct criminal activity, but also with a tool to undermine law enforcement’s ability to investigate that activity, identify and apprehend perpetrators, and rescue victims.

## **IV. What Strategies Can Be Employed to Meet These Challenges**

Combating offenders’ use of sophisticated techniques to hide their identity and location requires a multi-faceted approach. The global nature of online-facilitated crime in general, and sophisticated online crimes in particular, means that law enforcement must frequently collaborate with international partners to determine where criminal activity is occurring, as well as how evidence and criminal infrastructure can be seized so that perpetrators can be brought to justice. In recent years, coalitions of United States and foreign law enforcement agencies, frequently led by the Department of Justice, have seized numerous dark markets and other criminal facilities that rely on virtual currency to operate. In July 2017, for example, the Department announced a multinational effort that dismantled Alpha Bay, the largest criminal dark market then in operation. In February 2015, the FBI launched Operation Pacifier, discussed herein, which successfully interdicted a global child exploitation network. These operations followed the success of Operation Onymous, an international takedown in November 2014 of dozens of dark market websites, including the successor site to Silk Road (an online illicit drug marketplace), which itself was seized in October 2013.

Criminals’ use of advanced technology to obscure the identity and location of perpetrators and evidence means that law enforcement agencies must employ a variety of strategies—both ordinary and technical—to find and obtain evidence and identify and apprehend perpetrators. Even sophisticated criminals sometimes make mistakes. Determined, old-fashioned detective work may, in some instances, discover an error in a network or browser configuration that exposes the actual location of a Dark Web website or a clue that leads investigators to the actual identity of a perpetrator otherwise acting under an online alias. At the other end of the spectrum, investigators may be able to develop and deploy advanced tools and techniques that counteract criminals’ use of sophisticated technology, such as network investigative techniques (NITs), which can pierce the veil of anonymity offered by networks such as Tor and provide investigators with crucial, user-attributable information such as IP addresses.

In addition, legal authorities must be appropriately adapted to new and emerging technologies to ensure that advanced criminal schemes do not outpace the ability of law enforcement to appropriately utilize legal process and, where appropriate, conduct court-authorized searches, seizures or interceptions in order to interdict these schemes. One such adaptation occurred in December 2016, when FED. R. CRIM. P. 41 was amended to specifically authorize a magistrate judge “in any district where activities related to a crime may have occurred”<sup>1</sup> to issue a warrant “to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district” if “the district where the media or information is located has been concealed through technological means.”<sup>2</sup> This targeted, procedural amendment to the venue provisions of the Rule—which did not alter the probable cause or other Fourth Amendment requirements to obtain a warrant—can help ensure that technologies such as Tor do not render investigative abilities obsolete.

---

<sup>1</sup> FED. R. CRIM. P. 41(5).

<sup>2</sup> FED. R. CRIM. P. 41(6).

## V. FBI Operation Pacifier

FBI “Operation Pacifier” provides an illustrative example of how law enforcement sought to meet the significant challenges posed by a particular group of offenders’ use of anonymizing technology to perpetrate serious crimes on a massive global scale. “Operation Pacifier” targeted the administrators and users of “Playpen,” a highly-sophisticated, global enterprise dedicated to the sexual exploitation of children, organized via a members-only website that operated as a hidden service on the Tor network. Playpen’s administrators and more than 150,000 other members authored and viewed tens of thousands of postings relating to sexual abuse of children as young as infants and toddlers.

In February 2015, the “Playpen” web server was seized from a web-hosting facility in North Carolina. As noted above, because Playpen was a Tor hidden service, the seizure of the website did not provide law enforcement agents with IP address logs that could be used to identify site users, as well as the children they could have been abusing. Accordingly, it was necessary for the FBI to host, for a brief period, the Playpen website at an FBI facility in the Eastern District of Virginia, during which time the FBI obtained a search warrant to deploy a network investigative technique (“NIT”) and a Title III wiretap order to monitor user communications in an effort to identify those site users and children being victimized by them. The NIT warrant authorized the FBI to deploy the NIT—which consisted of computer code that, when deployed to a user’s computer, caused that computer to send to a government computer its actual IP address as well as a limited set of other, computer-related information—to Playpen users after they logged into the website. After obtaining that basic information via the NIT, additional investigation was conducted in an effort to determine the identity of the persons behind those computers and to search for and seize digital evidence, including the issuance of legal process regarding IP addresses obtained via the NIT and additional search warrants at premises associated with those IP addresses.

The results of the operation have been staggering in the United States and abroad—at least 348 United States arrests, the prosecution of at least fifty-one alleged hands-on child sex abusers, and the identification or rescue of at least fifty-five American children who were subjected to sexual abuse or exploitation; internationally, there have been at least 548 arrests and 296 children identified or rescued from sexual abuse or exploitation.

The Playpen administrators were successfully identified, apprehended and prosecuted as well. On September 16, 2016, a federal jury in the Western District of North Carolina convicted lead site administrator Steven W. Chase, fifty-seven, of Naples, Florida, of engaging in a child exploitation enterprise and related charges, and on May 1, 2017, he was sentenced to thirty years in prison and lifetime supervised release. Chase’s two co-defendants, fellow administrator Michael Fluckiger, forty-six, of Portland, Indiana, and global moderator David Lynn Browning, forty-seven, of Wootton, Kentucky, each pled guilty to engaging in a child exploitation enterprise and were respectively sentenced in January and February of 2017 to twenty years in prison and lifetime supervised release.

The myriad prosecutions related to Operation Pacifier brought to the forefront a number of complex legal issues. Defense strategies have largely focused on three litigation fronts: (1) motions to suppress evidence derived from the court-authorized NIT warrant; (2) motions to compel discovery regarding the investigation, primarily involving NIT “source code”; and (3) motions to dismiss indictments for purported “outrageous government conduct” because the Playpen website briefly operated on a law enforcement server. Although some of these challenges are particular to the scale and complexity of the Pacifier investigation, the strategy employed by defendants in these cases provides insight into the sort of tactics prosecutors can expect to face in other cases that involve anonymous networks and a combination of traditional and technical investigative techniques. While litigation in many cases remains ongoing, to date the government has successfully defended the investigation on all litigation fronts.

The Playpen NIT was deployed before the December 2016 Rule 41 amendment, described above, became effective. As such, many defendants have challenged the warrant authorizing the Playpen NIT, primarily claiming that the issuing magistrate lacked authority to issue it pursuant to the then-existing version of Rule 41, which purportedly rendered the warrant “*void ab initio*” and required suppression of evidence derived from the warrant. To date, three United States Courts of Appeal and more than seventy United States district court orders have denied such challenges, uniformly finding that, at a minimum, suppression of evidence derived from the Playpen NIT warrant is inappropriate under the *Leon* good-faith exception.<sup>3</sup> Numerous district courts have also found that the issuing magistrate had proper authority to issue the NIT warrant because it functioned as or similar to a digital tracking device.<sup>4</sup> The December 2016 Rule 41 amendment—which clarified the circumstances under which a particular magistrate may authorize a remote search of a computer whose location has been concealed through technological means—should largely eliminate such challenges to similar warrants in future investigations.

Some Pacifier defendants have also attempted to compel the government to provide internal Department of Justice or FBI memoranda related to the approval or conduct of the operation, and the computer “source code” related to the NIT. The government has successfully opposed production of that requested information: *first*, by providing substantial discovery to defendants in Pacifier cases (generally subject to protective order) to include IP address and other information collected by the NIT and the actual computer instructions that collected that information; *second*, by challenging the materiality of remaining requests for additional NIT or investigation-related information; and *third*, where appropriate, by contending that certain requested information (largely pertaining to the NIT source code) was subject to various privileges—including the common law “law enforcement privilege.”<sup>5</sup> Numerous courts have found requests for internal memoranda and NIT source code to be largely based upon a speculative foundation and, therefore, immaterial.<sup>6</sup> Some courts, in addition to a lack of materiality, have also found “source code” requests properly subject to the law enforcement privilege.<sup>7</sup>

Finally, some Pacifier defendants have moved to dismiss an indictment on the theory that it was so “outrageous” for the FBI to allow the Playpen site to briefly continue operating in order to identify users that any indictment returned against such a user should be dismissed. In response to such allegations, the government has persuasively articulated the justification for the court-authorized effort to

---

<sup>3</sup> To date, all of the district court orders that granted suppression motions regarding the Playpen NIT evidence have been overturned or occurred in a circuit that subsequently ruled suppression to be inappropriate. *See, e.g.*, *United States v. Levin*, 874 F.3d 316, 318 (1st Cir. 2017); *United States of America, v. Yang Kim*, also known as *Andrew Kim, Defendant.*, No. 16-CR-191 (PKC), 2017 WL 5256753 at 2 (E.D.N.Y. Nov. 10, 2017) (collecting cases).

<sup>4</sup> *See United States v. Leonard*, No. 17-CR-135, 2017 WL 4478330 at 3 (E.D. Va. Oct. 6, 2017).

<sup>5</sup> “The purpose of [the law enforcement privilege] is to prevent disclosure of law enforcement techniques and procedures, to preserve the confidentiality of sources, to protect witness and law enforcement personnel, to safeguard the privacy of individuals involved in an investigation, and otherwise to prevent interference with an investigation.” *In re The City of New York*, 607 F.3d 923, 940-41 (2d Cir. 2010) *quoting In re Dep’t of Investigation of City of New York*, 856 F.2d 481, 484 (2d Cir. 1988); *see also United States v. Cintolo*, 818 F.2d 980, 1002 (1st Cir. 1987) (noting that the privilege protects against divulging information that would allow criminals to develop countermeasures and techniques that frustrate lawful surveillance). Courts have held that the privilege prevents discovery of sensitive information about technologically sensitive law enforcement techniques and tools, such as NITs. *See United States v. Rigmaiden*, 844 F. Supp. 2d 982, 989, 993-1006 (D. Ariz. 2012) (description of sensitive investigative technologies); *United States v. Piroso*, 787 F.3d 358, 363-67 (6th Cir. 2015) (holding that source code of software used in an investigation is privileged); *United States v. Van Horn*, 789 F.2d 1492, 1507-08 (11th Cir. 1986) (holding that the nature and location of electronic surveillance equipment is privilege).

<sup>6</sup> *See, e.g.*, *United States v. Zak*, No. 16-CR-65-V, 2017 WL 4358140, 363-65 (W.D.N.Y. Oct. 2, 2017) (denying request for internal memoranda); *United States v. Cruz-Fajardo*, No. 1:16-CR-0014-TCB, 2017 WL 3634278 at 4 (N.D. Ga. Aug. 23, 2017) (denying request for NIT “source code”).

<sup>7</sup> *See, e.g.*, *United States v. Gaver*, No. 3:16-CR-88, 2017 WL 1134814 at 3 (S.D. Ohio Mar. 27, 2017).

identify sophisticated targets during a brief window of time, while carefully monitoring user communications and appropriately balancing investigative risks and benefits.<sup>8</sup> No court has granted such a motion.<sup>9</sup>

## VI. Conclusion

Technologically sophisticated offenders committing a variety of serious crimes via the Dark Web pose a significant, ongoing, and evolving threat to global public safety and law enforcement. To meet and overcome that threat, law enforcement will have to continue to coordinate globally, develop and deploy both ordinary and technical tools to identify perpetrators and seize evidence, and ensure that legal authorities are updated to prevent criminal schemes from outpacing law enforcement's ability to obtain legal process to further an investigation. If you have questions about Operation Pacifier or criminals' use of the Dark Web to facilitate child exploitation, please feel free to reach out to the Child Exploitation and Obscenity Section (CEOS) in the Criminal Division or your office's Project Safe Childhood (PSC) Coordinator. Other questions about investigating criminal activity on the Dark Web can be directed to the Computer Crime and Intellectual Property Section (CCIPS) in the Criminal Division or your office's Computer Hacking and Intellectual Property (CHIP) Coordinator. Additional resources regarding the issues discussed herein are available on the Criminal Division intranet.

### ABOUT THE AUTHORS

□ **Keith Becker** is a Deputy Chief with the Criminal Division's Child Exploitation and Obscenity Section (CEOS), where he has worked since 2010. From 2005 to 2010, he served as an Assistant United States Attorney for the District of Columbia, where he prosecuted federal and local cases involving violent crime, narcotics, and child pornography. He has co-authored four other United States Attorneys' Bulletin articles: "Whoever Knowingly Advertises: Considerations in Prosecuting Sex Trafficking," "Child Pornography Conspiracies in the Digital Age: A Primer," "Conspiracy and Internet Technology: Using the Child Exploitation Enterprise Statute to Prosecute Online Child Exploitation," and "Social Networking Site: Breeding Grounds for 'Sextortion' Prosecutions."

□ **Benjamin Fitzpatrick** is a Senior Counsel in the Computer Crime and Intellectual Property Section of the Criminal Division. Prior to joining CCIPS in 2015, he served as Senior Counsel in the Office of the Deputy Attorney General, working on national security issues, and was a Counsel in the Office of Law & Policy in the National Security Division. Before starting at DOJ in 2012, he was an attorney at Baker Botts, LLP, specializing in litigation and white-collar investigations.

<sup>8</sup> See e.g., *United States v. Kim*, No. 16-CR-191 (PKC), 2017 WL 394498 at 4 (E.D.N.Y. Jan. 27, 2017).

<sup>9</sup> See *id.* at 4-7 (collecting cases).

Page Intentionally Left Blank

# Expanding Victim Rights

*Katharine L. Manning*  
*Senior Attorney Advisor*  
*Executive Office for United States Attorneys*  
*Office of Legal and Victim Programs*

## I. Introduction

It has been more than thirteen years since Congress passed the Crime Victims' Rights Act, 18 U.S.C.A. § 3771 (hereinafter CVRA). In that time, courts have applied the statute to expand the victims' role in the courtroom, at times broadly interpreting the statute's language so as to give effect to its larger purpose: ensuring victims the ability to participate in federal criminal cases. In this article, I will review some of those cases, focusing in particular on the victims' rights to protection from the accused, not to be excluded from court proceedings, to be heard, to proceedings free from delay, and to privacy.

## II. The Right to Protection

The CVRA's first 'right' is to reasonable protection from the accused.<sup>1</sup> As noted by the Act's Senate sponsor:

“The placement of this right as the first right is quite deliberate. Senator Feinstein thought the right so important that she directed during the drafting that it be moved from paragraph 2 of the lists of rights in the VRRRA to paragraph 1 of the new law. This placement reinforces the principle that government's first and foremost obligation to its citizens is to protect them—especially those who already have been victims of a crime.”<sup>2</sup>

Prior to the CVRA's enactment, the sole remedy for a victim who was harassed by a defendant awaiting trial was for the government to file an application for a civil protection order under 18 U.S.C.A. § 1514. This application must be accompanied by an affidavit or verified complaint, and requires a hearing at which both sides may present evidence and cross-examine witnesses.<sup>3</sup>

One prosecutor used the CVRA's right to protection to obtain a no-contact order in a much more streamlined fashion. In *United States v. Darcy*, the defendant, who was incarcerated while awaiting trial, sent multiple letters to his minor victim.<sup>4</sup> When the child's mother requested assistance, the prosecutor moved the court for an order of protection under the CVRA.<sup>5</sup> The court imposed a stay-away order under penalty of contempt pursuant to the CVRA's right to protection instead of requiring the more cumbersome filing of a motion for a civil protection order under 18 U.S.C.A. § 1514.<sup>6</sup>

---

<sup>1</sup> 18 U.S.C.A. § 3771(a) (West 2012).

<sup>2</sup> The Honorable Jon Kyl, Steven J. Twist, Stephen Higgins, The Honorable Jon Kyl et. al., *On the Wings of Their Angels: The Scott Campbell, Stephanie Roper, Wendy Preston, Louarna Gillis, and Nila Lynn Crime Victims' Rights Act*, 9 LEWIS & CLARK L. REV. 581, 595 (2005).

<sup>3</sup> 18 U.S.C.A. § 1514 (a)(1), (b).

<sup>4</sup> *United States v. Darcy*, 2009 WL 1628885 at 1 (W.D.N.C. June 10, 2009).

<sup>5</sup> *Id.*

<sup>6</sup> *Id.*

### III. The Right Not to Be Excluded

Victims also have a right not to be excluded from public court proceedings absent a finding that their testimony would be materially altered if they heard other testimony at the proceeding.<sup>7</sup>

The sequestration requirements of Federal Rule of Evidence 615 and similar state rules meant that many victims were barred from the courtroom as a matter of course, which was devastating to many victims. As one mother of a homicide victim put it, “[i]nstead of hearing the truth and seeing justice imposed, for six weeks we were banished from the most important event of our lives, and made to feel like second-class citizens.”<sup>8</sup> The CVRA is a bulwark against such treatment and an exception to Rule 615’s rule of exclusion.<sup>9</sup>

Courts interpreting this right have worked to give effect to its broader purpose. For instance, in *United States v. Hertz*, the defendant filed a motion to change the venue from Boulder, Colorado, where the crime occurred and where the victims resided, to the Eastern District of Washington, where he lived, delineating his health issues and travel expenses.<sup>10</sup> Nothing in the CVRA grants victims a right to be heard on a motion to change venue. Indeed, the impact of a transfer on the victims is not even generally included on the list of factors to be considered when deciding a transfer motion.<sup>11</sup> In considering the motion, though, the court in *Hertz* gave consideration to the CVRA’s rights to be present and heard at proceedings, and to the obligation the CVRA places on courts to “make every effort to permit the fullest attendance possible by the victim.”<sup>12</sup> The court then noted that, were the action transferred, the victims would incur the same challenges in attending that the defendant himself identified as a hardship. The court went on that, “[t]he Defendant’s motion offers no explanation why, as between himself and the victims of his actions, the victims should be required to bear the burdens of travel expense and inconvenience in order to attend court proceedings in this case.”<sup>13</sup> The motion was denied.

Similarly, in *United States v. Larsen*, the defendant moved to transfer the case, involving securities fraud of three individuals in Rockland County, New York, to the Middle District of Pennsylvania, where the defendant resided.<sup>14</sup> After considering each of the Platt factors, the court noted that, while neither party had raised the issue, the convenience of the victims, too, “weigh[ed] in favor of keeping the case in New York . . .” as none of the victims lived in the Middle District of Pennsylvania, and at least two resided in New York.<sup>15</sup> The court further noted that the victims’ rights to proceedings free from unreasonable delay and restitution would be better served by denying the transfer and allowing the case to proceed.<sup>16</sup>

Courts have also been willing to use technology to permit victims to be present at proceedings that they otherwise would not have been able to attend. In *United States v. Benson*, where out-of-state

---

<sup>7</sup> 18 U.S.C.A. § 3771(a)(3) (West 2012).

<sup>8</sup> Douglas E. Beloof & Paul G. Cassell, *The Crime Victim's Right to Attend the Trial: The Reascendant National Consensus*, 9 LEWIS & CLARK L. REV. 481, 503 (2005) (statement of Roberta Roper, who went on to found the Maryland Crime Victims’ Resource Center).

<sup>9</sup> See *United States v. Edwards*, 526 F.3d 747, 757-58 (11th Cir. 2008); *In re Mikhel*, 453 F.3d 1137, 1138-39 (9th Cir. 2006).

<sup>10</sup> *United States v. Hertz*, 2010 WL 447749 at 1 (D. Colo. Feb. 4, 2010).

<sup>11</sup> See *Platt v. Minnesota Min. & Mfg. Co.*, 376 U.S. 240, 243-44 (1964). Note, however, that FED. R. CRIM. P. 21(b) allows the court to consider a transfer for the convenience of victims.

<sup>12</sup> *Hertz*, 2010 WL 447749 at 3.

<sup>13</sup> *Id.*

<sup>14</sup> *United States v. Larsen*, 2014 WL 177411 at 1-2 (S.D.N.Y. Jan. 16, 2014).

<sup>15</sup> *Id.* at 4.

<sup>16</sup> *Id.* See also *United States v. Agriprocessors, Inc.*, 2009 WL 721715 at 2 (N.D. Iowa Mar. 18, 2009) (citing the impact on victims as a reason to deny transfer motion).

victims wanted to participate in a revocation hearing, the court allowed them to attend the proceeding by telephone conference call.<sup>17</sup> Anecdotal reports from across the country indicate that other courts have allowed victims to attend proceedings via conference call and speakerphone as well.

## IV. The Right to Be Heard

The CVRA gives victims the right to be reasonably heard at public proceedings in the district court involving release, plea, sentencing, or parole.<sup>18</sup> The Ninth Circuit found that this right provides victims “an infeasible right to speak, similar to that of the defendant . . .”<sup>19</sup> The Kenna court, in finding that the CVRA guarantees that victims have the right to speak where they prefer to, and that the court’s allowing a written statement would not accord the right, noted that the CVRA

“[W]as enacted to make crime victims full participants in the criminal justice system. Prosecutors and defendants already have the right to speak at sentencing . . . ; our interpretation puts crime victims on the same footing. Our interpretation also serves to effectuate other statutory aims: (1) To ensure that the district court doesn’t discount the impact of the crime on the victims; (2) to force the defendant to confront the human cost of his crime; and (3) to allow the victim “to regain a sense of dignity and respect rather than feeling powerless and ashamed.”<sup>20</sup>

In a series of recent decisions, courts have removed procedural hurdles to victims allocuting at sentencing. For instance, in *United States v. Grigg*, the defendant challenged his sentence because the district court had not sworn in victims prior to hearing their statements.<sup>21</sup> The Sixth Circuit held that “[t]here is no such requirement in the CVRA.”<sup>22</sup> Further, the court noted,

“Every court that has examined this issue has held that there is no requirement to swear in CVRA victims. See *United States v. Myers*, 402 Fed. Appx. 844, 845 (4th Cir. 2010); *United States v. Shrader*, No. 1:09-0270, 2010 WL 4781625, at \*3 (S.D. W.Va. Nov. 16, 2010) (“It is apparent that a victim has the right to speak at sentencing about the impact a defendant’s criminal conduct has had upon her without being placed under oath and cross examined just as a defendant has the right to allocute in mitigation of sentence.”); *United States v. Marcello*, 370 F.Supp.2d 745, 750 (N.D. Ill. 2005) (“Given changes in the *Federal Rules of Criminal Procedure*, victims have a right to speak in open court in a manner analogous to the defendant’s personal right of allocution at sentencing . . . Today, both defendant and victim have the right to speak without being sworn as a witness before sentence is passed.”<sup>23</sup>

Similarly, courts have held that a victim impact statement need not be a sworn statement.<sup>24</sup>

Finally, the Fifth Circuit held that a defendant’s due process rights were not violated where the court denied him the ability to cross-examine a victim who was allocuting at sentencing.<sup>25</sup> The court found that, “[d]ue process merely requires that information relied on in determining an appropriate

---

<sup>17</sup> *United States v. Benson*, 2014 WL 2705227 at 3 (N.D. Cal. June 13, 2014).

<sup>18</sup> 18 U.S.C.A. § 3771(a)(4).

<sup>19</sup> *Kenna v. U.S. Dist. Court for C.D.Cal.*, 435 F.3d 1011, 1016 (9th Cir. 2006).

<sup>20</sup> *Id.* quoting Jayne W. Barnard, *Allocation for Victims of Economic Crimes*, 77 NOTRE DAME L. REV. 39, 41 (2001).

<sup>21</sup> *United States v. Grigg*, 434 F. App’x 530, 533 (6th Cir. 2011).

<sup>22</sup> *Id.*

<sup>23</sup> *Id.* at 533-34 (internal citations omitted).

<sup>24</sup> See *United States v. Bolze*, 444 F. App’x 889, 891-92 (6th Cir. 2012), and *Myers*, 402 F. App’x at 845.

<sup>25</sup> See *United States v. Castillo*, 476 F. App’x 774, 775 (5th Cir. 2012).

sentence have some minimal indicium of reliability and bear some rational relationship to the decision to impose a particular sentence . . . Also, the Confrontation Clause does not apply to sentencing hearings . . . In fact, a district court may rely upon uncorroborated hearsay in making sentencing determinations.”<sup>26</sup>

In another line of cases, courts have held that it was not a violation of a plea agreement where the prosecutor agreed to recommend a specific sentence, but a victim’s statement at sentencing persuaded the court to impose a higher sentence. *United States v. Castaldi* involved a Ponzi scheme with losses totaling roughly \$40 million.<sup>27</sup> As part of the plea, the government agreed to a Sentencing Guidelines range of 151 to 188 months in prison, and to recommend a sentence on the lower end of the range.<sup>28</sup> At the sentencing hearing, the court acknowledged that it had received and considered sentencing memoranda from the prosecutor and defense, both arguing for a sentence in the lower range.<sup>29</sup> The court then read from some of the many victim impact statements it had received.

To describe these letters as compelling is an understatement. Victims described how Castaldi had deprived them of their life savings, college money for their children, money saved for retirement, money saved to start a business, money for medical care, and the life insurance money when a spouse died. One of Castaldi’s last victims described how he convinced her family to take out a new mortgage for \$200,000 and invest it with him in late 2008, meaning it was lost. One letter pointed out that on November 15, 2008, when Castaldi knew his scheme was collapsing, he conned his own 92-year-old aunt to “invest” \$120,000 with him so she could pay a care-giver with the interest. The aunt’s money was also lost, of course.<sup>30</sup> The court then received oral statements from victims, which “were similar in content and power to the victims’ letters.”<sup>31</sup>

In imposing a sentence, the trial court noted that Castaldi’s actions “had a horrific impact on the victims. And that impact must be considered in imposing a sentence that promotes respect for the law and provides just punishment.”<sup>32</sup> The court sentenced Castaldi to the maximum possible sentence under the agreed Guidelines range, with consecutive sentences, for a total of 276 months in prison.<sup>33</sup>

The Seventh Circuit upheld the sentence, finding it both obvious and appropriate that the trial court was swayed by the victim impact statements: “The judge’s explanation emphasized so strongly the harm to the victims that we know that factor dominated his thinking.”<sup>34</sup>

---

<sup>26</sup> *Id.* (internal citations and quotations omitted); *see also* *United States v. Barouch*, 2013 WL 2151226 at 9 (N.D. Tex. May 17, 2013) (“The victim thus has the right to make a statement at sentencing about the effect the defendant’s criminal conduct had on her without being cross-examined or placed under oath, just as a defendant has the right to make whatever statement he wants in mitigation”).

<sup>27</sup> *United States v. Castaldi*, 743 F.3d 589, 591 (7th Cir. 2014).

<sup>28</sup> *Id.* at 592.

<sup>29</sup> *Id.* at 593.

<sup>30</sup> *Id.*

<sup>31</sup> *Id.*

<sup>32</sup> *Id.* at 594.

<sup>33</sup> *Id.* at 594-95.

<sup>34</sup> *Id.* at 596. *See also* *United States v. Aguiard*, 476 F. App’x 8, 9 (5th Cir. 2012) (court imposed the statutory maximum sentence of twenty years in part because “it had determined that the case was unique in light of the devastating financial and emotional impact on the victims and their families”); *United States v. Brown*, 629 Fed. App’x 793, 795 (9th Cir. Oct. 30, 2015) (in presenting victim impact testimony, the government did not breach the plea agreement, but was “simply fulfilling its statutory obligations under the Crime Victims’ Rights Act”). Note, however, that where the government presented a letter from a co-defendant’s family member arguing against a sentence reduction, it was found to be a violation of a post-conviction agreement. *See* *United States v. Rausini*, 517 F. App’x 587, 588 (9th Cir. 2013) (“The letter did not fall under the Crime Victims’ Rights Act, as asserted by the

## V. Proceedings Free from Delay

While defendants have the constitutional right to a speedy trial, prior to the CVRA, victims had no analogous protection when defendants sought to delay proceedings. “[D]elays in criminal proceedings are among the most chronic problems faced by victims. Whatever peace of mind a victim might achieve after a crime is too often inexcusably postponed by unreasonable delays in the criminal case.”<sup>35</sup> The CVRA’s right to proceedings free from unreasonable delay addresses this concern.<sup>36</sup>

In *United States v. Abrams*, the defendant had already been granted two continuances, as well as a motion for new counsel, and then a motion to proceed in pro per.<sup>37</sup> The court denied the defendant’s third motion for continuance, noting “the Government’s concerns regarding the impact of delay on the victims involved in the trial.”<sup>38</sup>

## VI. Respect for Dignity and Privacy

Courts have also made great strides in protecting victims through the CVRA’s right to be treated with fairness and with respect for the victim’s dignity and privacy.<sup>39</sup> As noted in the CVRA’s legislative history, “[t]he broad rights articulated in this section are meant to be rights themselves and are not intended to just be aspirational.”<sup>40</sup> In a variety of contexts, courts have given meaning to this right, allowing victims to maintain privacy and dignity in criminal cases.<sup>41</sup>

Often, this right is used to protect private victim information that is sought by the defendant. For instance, in *United States v. Rand*, the defendant was charged with production, receipt, and possession of child pornography, as well as enticement, with four victims ranging in age from eleven to sixteen.<sup>42</sup> In a pretrial motion, the defendant argued that it was “wholly inconsistent” for the court to order him to produce non-child pornography from his electronic media, while his fourteen-year-old victim was not ordered to produce non-contraband images of herself and her family from her own phone.<sup>43</sup> Quoting from the government’s brief, the court noted that “[i]f an electronic copy of this evidence is taken outside government control, there is no ability to ensure what may happen to those images, whether they may be altered in some manner or duplicated or used in any manner to harass the victim.”<sup>44</sup> The court denied the

---

government before the district court, because the author of the letter was not a family member of one of the victims”).

<sup>35</sup> 9 LEWIS & CLARK L. REV., at 612.

<sup>36</sup> 18 U.S.C.A. § 3771(a)(7).

<sup>37</sup> *United States v. Abrams*, 2016 WL 107945 at 1 (D. Nev. Jan. 8, 2016).

<sup>38</sup> *Id.* at 2. *See also* *Larsen*, 2014 WL 177411 at 4 (denying motion for transfer in part due to concerns about the delay the transfer would cause); *United States v. Martinez*, 2013 WL 11318858 at 2 (E.D. Wash. Nov. 20, 2013) (denying motion to continue due in part to “the alleged victim’s family’s objection and rights to proceedings free of unreasonable delay.”); *United States v. LeRoy*, 2017 WL 2938199 at 3 (W.D. Pa. July 10, 2017) (denying motion for new trial where “minor victims have a vital and statutorily protected interest in the timely conclusion of this criminal proceeding, as the minor victims therapeutic needs assessment establish severe, negative repercussions that may go un-remedied if the Court were to grant Defendant’s untimely Motion.”).

<sup>39</sup> 18 U.S.C.A. § 3771(a)(8).

<sup>40</sup> 150 Cong. Rec. S4269 (daily ed. Apr. 22, 2004) (statement of Sen. Kyl).

<sup>41</sup> While this article focuses on the CVRA, those working with child victims and witnesses should make note of the enhanced privacy protection of 18 U.S.C.A. § 3509 (West).

<sup>42</sup> *United States v. Rand*, 2011 WL 4949695 at 1 (S.D. Fla. Oct. 18, 2011).

<sup>43</sup> *Id.* at 4.

<sup>44</sup> *Id.*

motion, citing the affirmative obligation the CVRA places on the court and on the prosecutor to ensure that the victim's right to be treated with respect for her dignity and privacy.<sup>45</sup>

Similarly, in *United States v. Gatewood*, a man accused of multiple sexual assaults in Indian Country filed a motion to compel after the government redacted victim names and contact information before producing documents to him.<sup>46</sup> Citing the CVRA, the court denied the motion, noting that "the relevant statutes state a duty to withhold much of the currently redacted information on privacy grounds."<sup>47</sup>

The defendant in *United States v. Shrader* sought a subpoena for the victim's counseling records, arguing that the victim had waived the psychotherapist patient privilege by seeking victim compensation for the costs of the treatment and, thus, the defendant should be able to use the information in the therapist's file to help him at sentencing.<sup>48</sup>

The right to privacy has also been used by courts in denying motions by the press for access to private victim information in cases. *United States v. Patkar*<sup>49</sup> and *United States v. Robinson*<sup>50</sup> are both extortion cases where the court, relying on the CVRA, denied the press access to the information that was the subject of the extortion. Allowing the press access to such information, the *Patkar* court held, would mean the defendant "would be free to disclose the very material that formed the basis of his extortion."<sup>51</sup>

In *United States v. Madoff*, the press sought access to emails the victims had sent to prosecutors, describing the impact of the crime and asking for an opportunity to be heard at the change of plea hearing.<sup>52</sup> The United States Attorney's Office filed the emails under seal, but the press requested the full text of the emails without redactions.<sup>53</sup> Relying on the CVRA, the court ordered that emails from those victims who requested privacy remain under seal.<sup>54</sup> Noting that the court must balance the press right of access against the privacy rights of victims, the *Madoff* court stated that, "[t]he privacy interests of innocent third parties . . . should weigh heavily in a court's balancing equation."<sup>55</sup>

Similarly, in *United States v. Belfort*, a television producer sought a list of victim names and the amounts of restitution they were each awarded.<sup>56</sup> Noting that the information sought was not generally considered public information, and relying on the CVRA's right to privacy, the court held that, "the interest in protecting the victims' privacy significantly outweighs the relatively low presumption of access to the document."<sup>57</sup>

## VII. Conclusion

As noted by the court in *Patkar*, the CVRA "was intended to provide meaningful rights, and not a simple laundry list of aspirational goals as to how the government and courts should treat victims."<sup>58</sup> I

---

<sup>45</sup> *Id.*

<sup>46</sup> *United States v. Gatewood*, 2012 WL 2286999 at 1 (D. Ariz. June 18, 2012).

<sup>47</sup> *Id.* at 2.

<sup>48</sup> *Shrader*, 2010 WL 4781625 at 1.

<sup>49</sup> *United States v. Patkar*, 2008 WL 233062 (D. Haw. Jan. 28, 2008).

<sup>50</sup> *United States v. Robinson*, 2009 WL 137319 (D. Mass. Jan. 20, 2009).

<sup>51</sup> *Patkar*, 2008 WL 233062 at 6.

<sup>52</sup> *United States v. Madoff*, 626 F. Supp. 2d 420, 422 (S.D.N.Y. 2009).

<sup>53</sup> *Id.*

<sup>54</sup> *Id.* at 425.

<sup>55</sup> *Id.* at 424 (citation omitted).

<sup>56</sup> *United States v. Belfort*, 2014 WL 2612508 at 1 (E.D.N.Y. June 11, 2014).

<sup>57</sup> *Id.* at 4. *See also* *United States v. Starr*, 2011 WL 1796340, at 2 (S.D.N.Y. May 2, 2011) (denying newspaper's request for victims' restitution requests).

<sup>58</sup> *Patkar*, 2008 WL 233062 at 5.

encourage prosecutors to use these rights where appropriate to protect victims' interests and to ensure victims a role in the criminal justice process.

#### **ABOUT THE AUTHOR**

□ **Katharine L. Manning** is a Senior Attorney Advisor with the Executive Office for United States Attorneys' Office of Legal and Victim Programs. Since 2004, she has worked to implement the Crime Victims' Rights Act, the Victims' Rights and Restitution Act, and the Attorney General Guidelines for Victim and Witness Assistance within the Justice Department. Her previous USA Bulletin articles are on the Conundrum of Victim Rights in Conspiracy Cases (July 2013) and on Guardians ad Litem and Victim Counsel in Cases with Child Victims (July 2015).

Page Intentionally Left Blank

# When Attorney-Client Communication is Not Privileged: Invoking the Crime-Fraud Exception in Grand Jury Investigations

*Gretchen C. F. Shappert*  
*U.S. Attorney for the Virgin Islands*

## I. Introduction

### A. Hypotheticals

- Corporate counsel advises a corporate officer that corporate emails are being retained as part of an ongoing federal investigation and that she should retain her emails. It later comes to the attention of federal agents that the corporate officer attempted to delete emails after she was advised of the ongoing investigation. Can the grand jury compel corporate counsel to testify about his conversations with the corporate officer and to disclose his notes regarding the conversation?<sup>1</sup>
- During trial in a federal firearms case, the government becomes suspicious that one of the defense exhibits, the photocopy of a document, is fraudulent. After the trial, the government's suspicions are confirmed. Can defense counsel and her investigator be compelled to testify before the grand jury? Additionally, what is the scope of questions that they may be asked?<sup>2</sup>
- An American corporation is working a large financial deal with a foreign bank. There is a delay in the process. The corporate president seeks legal advice from an independent lawyer who works in the corporation's office space about a possible payment to a bank official in order to facilitate the deal. The lawyer warns that the payment may implicate the Federal Corrupt Practices Act, and the corporate president disagrees. When federal agents later learn that the corporate president made a payment to the bank officer's sister, can the grand jury compel the lawyer to testify about his conversation with the corporation's president?<sup>3</sup>

Each of these examples is a real-life situation involving application of the crime-fraud exception in a federal grand jury proceeding which will be discussed in this article. Effective use of the crime-fraud exception enables the grand jury to consider important evidence that would otherwise be shielded by the attorney-client privilege. It prevents criminals, fraudsters, and the occasional malevolent attorney from obstructing the grand jury process. Finally, it supports and reinforces the impartial administration of justice.

---

<sup>1</sup> In re Grand Jury Investigation, 445 F.3d 266 (3d Cir. 2006).

<sup>2</sup> In re Grand Jury Subpoena, 870 F.3d 312 (4th Cir. 2017).

<sup>3</sup> In re Grand Jury Subpoena, 745 F.3d 681 (3d Cir. 2014).

## B. The Federal Grand Jury and the Attorney-Client Privilege

The federal grand jury occupies an essential role in the United States criminal justice system. The grand jury serves a vital function of “determining if there is probable cause to believe that a crime has been committed and of protecting citizens against unfounded criminal prosecutions.”<sup>4</sup> The grand jury’s investigative powers to subpoena witnesses and collect evidence are necessarily broad. In the context of the grand jury, the longstanding principle that the public has a right to every person’s evidence is particularly strong.<sup>5</sup> A court will intervene only when a recognized privilege provides legitimate grounds for refusing to comply with a grand jury subpoena.<sup>6</sup> Recognized privileges are protected by the Constitution, common law, or statute.<sup>7</sup> The attorney-client privilege is the oldest of the privileges for confidential communications acknowledged in the common law.<sup>8</sup>

The attorney-client privilege is intended to protect confidential communications between clients and their counsel, “to encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice.”<sup>9</sup> As a general rule, the burden is on the party asserting the privilege to establish the privilege claim.<sup>10</sup> When the client or the putative client claims the privilege, he or she must demonstrate that: (1) the asserted holder of the privilege is or sought to become a client; (2) the person to whom the communication was delivered (a) is a member of the bar of the court or the bar member’s subordinate, and (b) in connection with the communication is acting as an attorney; (3) the communication pertains to a fact of which the attorney was advised (a) by the client, (b) without the presence of strangers, (c) for the purpose of obtaining primarily either (i) an opinion on the law, or (ii) legal services, or (iii) assistance in some legal proceeding, and not (d) for the purpose of committing a crime or tort; and (4) the privilege has been (a) claimed and (b) not waived by the client.<sup>11</sup>

## C. The Attorney-Client Privilege and the Crime-Fraud Exception

The attorney-client privilege allows an attorney to refuse to testify or to have his client testify as to confidential communications between the two made in connection with the rendering of legal representation.<sup>12</sup> However, the privilege is not absolute, and communications are not privileged “where the desired advice refers not to prior wrongdoing, but to future wrongdoing.”<sup>13</sup> The question is “whether the client’s purpose is the furtherance of a future fraud or crime.”<sup>14</sup> If the client intends to further a future fraud or crime, it does not matter whether the attorney is aware of the future crime or not.<sup>15</sup> Thus, “[i]f

<sup>4</sup> *Branzburg v. Hayes*, 408 U.S. 665, 686-87 (1972).

<sup>5</sup> *Id.* at 688.

<sup>6</sup> *In re Sealed Case*, 676 F.2d 793, 806 (D.C. Cir. 1982).

<sup>7</sup> *Branzburg*, 408 U.S. at 688, *citing* *United States v. Bryan*, 339 U.S. 323, 331 (1950).

<sup>8</sup> *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981); *In re Grand Jury Proceedings #5 Empanelled Jan. 28, 2004*, 401 F.3d 247, 250 (4th Cir. 2005).

<sup>9</sup> *Upjohn Co.*, 449 U.S. at 389.

<sup>10</sup> *See In re Grand Jury Subpoena (Mr. S.)*, 662 F.3d 65, 69 (1st Cir. 2011) (“The burden of showing that documents are privileged rests with the party asserting the privilege.”).

<sup>11</sup> *United States v. Moazzeni*, 906 F. Supp.2d 505, 511 (E.D. Va. 2012), *quoting* *N.L.R.B. v. Interbake Foods, LLC*, 637 F.3d 492, 501-02 (4th Cir. 2011) (citations omitted).

<sup>12</sup> *In re Grand Jury Proceedings*, 417 F.3d 18, 21 (1st Cir. 2005); *Cavallaro v. United States*, 284 F.3d 236, 245 (1st Cir. 2002).

<sup>13</sup> *United States v. Zolin*, 491 U.S. 554, 562-63 (1989) (quoting 8 *Wigmore*, § 2298, at 573); *United States v. Martin*, 278 F.3d 988, 1001 (9th Cir. 2002); *In re John Doe, Inc.*, 13 F.3d 633, 636 (2d Cir. 1994).

<sup>14</sup> *In re Grand Jury Proceedings*, 43 F.3d 966, 972 (5th Cir. 1994), *citing from* 1 *McCormick on Evidence* § 95, at 350 (John William Strong ed., 4th ed. 1992).

<sup>15</sup> *In re Grand Jury Proceedings #5 Empanelled January 28, 2004*, 401 F.3d at 251; *In re BankAmerica Corp. Sec. Litig.*, 270 F.3d 639, 641-42 (8th Cir. 2001); *In re Grand Jury Proceedings*, 87 F.3d 377, 378 (9th Cir. 1996). *See*

there is a prima facie showing that the professional relationship was intended to further a criminal enterprise, the privilege does not exist.”<sup>16</sup> The crime-fraud exception, one of several qualifications of the attorney-client privilege, vitiates the attorney-client privilege where the client sought or retained legal counsel in order to commit or facilitate a crime or fraud.<sup>17</sup>

The attorney-client privilege and the crime-fraud exception are the product of federal common law “interpreted by the United States courts in the light of reason and experience.”<sup>18</sup> The Supreme Court has held that in camera review may be used to determine whether the allegedly privileged attorney-client communications fall within the crime-fraud exception.<sup>19</sup> Before the district court may commence an in camera review of allegedly privileged communications at the request of the party opposing the privilege, that party must present evidence sufficient to support a reasonable belief that the in camera review may elicit evidence establishing the applicability of the crime-fraud exception.<sup>20</sup> The threshold to obtain an in camera review may be satisfied by using any relevant evidence lawfully obtained that has not been adjudicated to be privileged, even in if the evidence is not independent of the allegedly privileged communications.<sup>21</sup>

When prosecutors invoke the crime-fraud exception during a grand jury investigation, the government must make a showing that: (1) the client was engaged in or planning criminal or fraudulent activity when the communications occurred; and (2) that the communications with counsel were intended by the client to further or conceal the criminal or fraudulent activity.<sup>22</sup> The government is not required to “prove the crime or fraud” at the grand jury stage; rather, “the proof ‘must be such as to subject the opposing party to the risk of non-persuasion if the evidence as to the disputed fact is left unrebutted.’”<sup>23</sup>

Grand jury proceedings, of course, are closed and secret.<sup>24</sup> Facts supporting evidence of the crime-fraud exception and even the nature of the alleged crime or fraud itself may be presented ex parte to a district court and held in confidence.<sup>25</sup> The government must merely make a threshold showing “of a

---

United States v. Hodge & Zweig, 548 F.2d 1347, 1354 (9th Cir. 1977) (“The crime or fraud exception applies even where the attorney is completely unaware that his advice is sought in furtherance of such an improper purpose.”).

<sup>16</sup> In re Grand Jury Proceedings in Matter of Fine, 641 F.2d 199, 203 (5th Cir. 1981), *quoting* Hodge and Zweig, 548 F.2d at 1354.

<sup>17</sup> In re Grand Jury Proceedings, 802 F.3d 57, 65 (1st Cir. 2015); In re Grand Jury Proceedings, 417 F.3d at 22.

<sup>18</sup> FED. R. EVID. 501.

<sup>19</sup> Zolin, 491 U.S. at 574.

<sup>20</sup> *Id.* at 574-75.

<sup>21</sup> *Id.* at 572-73.

<sup>22</sup> In re Grand Jury Proceedings, 802 F.3d at 65-66, *citing* In re Grand Jury Proceedings (Gregory P. Violette), 183 F.3d 71, 75 (1<sup>st</sup> Cir. 1999). *See* In re Grand Jury Proceedings #5 Empanelled January 28, 2004, 401 F.3d at 251. *See also* In re Grand Jury Proceedings, 417 F.3d at 23-25 (noting that application of the crime-fraud exception requires evidence of the individual client’s *use or aim to use* the lawyer to foster the crime or fraud in a case involving a joint-defense agreement and multiple groups of clients).

<sup>23</sup> In re Grand Jury Proceedings #5, 401 F.3d at 251, *quoting* Duplan Corp. v. Deering Milliken, Inc., 540 F.2d 1215, 1220 (4th Cir. 1976).

<sup>24</sup> FED. R. CRIM. P. 6.

<sup>25</sup> In re Grand Jury Proceedings, Thursday Special Grand Jury Sept. Term, 1991, 33 F.3d 342, 352-53 (4th Cir. 1994), *citing* In re Grand Jury Subpoena, 884 F.2d 124 (4th Cir. 1989). *See also* In re Grand Jury Subpoena, 223 F.3d 213, 219 (3d Cir. 2000) (“We today join the ranks of our sister circuits in holding that it is within the district courts’ discretion, and not violative of due process, to rely on an *ex parte* government affidavit to determine that the crime-fraud exception applies and thus compel a target-client’s subpoenaed attorney to testify before the grand jury); In re Grand Jury Subpoena as to C97-216, 187 F.3d 996, 998 (8<sup>th</sup> Cir. 1999) (there was no plain error in district court’s use of sealed *ex parte* affidavit in determining whether the government had made a threshold showing to justify in camera examination of the client’s former attorney to determine if the crime-fraud exception applied; citing other circuit decisions).

factual basis adequate to support a good faith belief by a reasonable person that in camera review of the materials may reveal evidence to establish the claim that the crime-fraud exception applies.”<sup>26</sup>

## **II. Making the Necessary Showing for the Crime-Fraud Exception: In Camera and Ex Parte Review and the Proper Scope of the Exception**

When federal prosecutors believe that the target or a potential target of a grand jury investigation has used the services of an attorney to further a continuing or future crime or fraud, how does the government make the necessary showing to override the attorney-client privilege?<sup>27</sup> The Supreme Court’s analysis in *United States v. Zolin* offers important practical guidance as to what evidence the district court may consider. *Zolin* involved an Internal Revenue Service (IRS) investigation of the tax returns of L. Ron Hubbard, founder of the Church of Scientology (the Church). In the course of its investigation, the IRS issued a summons to the Clerk of Court, demanding access to documents filed in a State of California civil case involving the Church, including audiotapes. Some of the documents in the state case had been filed under seal. The Church and Hubbard’s widow intervened and obtained a temporary restraining order from the District Court in the Central District of California. The IRS, in turn, filed a petition in federal court to enforce its summons, and the Church and Hubbard’s widow intervened to oppose production on grounds of lack of relevance and the attorney-client privilege.<sup>28</sup>

The IRS argued that the tapes fell within the crime-fraud exception and urged the District Court to listen to the tapes in the course of making its privilege determination. The Ninth Circuit opined that determination of the applicability of the crime-fraud exception must be based on sources independent of the attorney-client communications memorialized on the tapes. The Supreme Court, however, concluded that this was error, and that “a rigid independent evidence requirement does not comport with ‘reason and experience’ . . . that in camera review may yield evidence that establishes the exception’s applicability.”<sup>29</sup> The threshold showing to obtain in camera review is satisfied by using any relevant, lawfully obtained evidence that has not been adjudicated as privileged, even where the evidence is not independent of the allegedly privileged communications.<sup>30</sup>

An excellent example of in camera review of an attorney’s legal advice is a recent Third Circuit decision, *In re Grand Jury Subpoena*, arising from a grand jury investigation of a Pennsylvania corporate consulting firm accused of making bribes to obtain business in violation of the Foreign Corrupt Practices Act (FCPA).<sup>31</sup> The president of the corporation approached an attorney for legal advice who worked out of the corporation’s office but practiced law independently. The corporation president told the lawyer that he planned to pay a banker associated with a corporation project in order to ensure that the project proceeded swiftly, as the banker was threatening to delay the project’s approval. Based upon his initial legal research and the possibility that the FCPA was applicable, and that the foreign bank was possibly a government entity and the banker a government official, the attorney advised the president not to make the payment. Insisting that the payment was legal and did not violate the FCPA, the president stated that

---

<sup>26</sup> *Zolin*, 491 U.S. at 572. (Internal quotation and citation omitted).

<sup>27</sup> *Id.*, See generally, *United States v. Boender*, 649 F.3d 650, 656 (7th Cir. 2011) (“The rule allowing for *in camera* review does not presuppose any particular quantum of evidence establishing the appropriateness of the [crime-fraud] exception itself, merely enough evidence to support a ‘good faith belief by a reasonable person’ that such review may reveal evidence establishing the exception.”).

<sup>28</sup> *Zolin*, 491 U.S. at 557-58.

<sup>29</sup> *Id.* at 574-75.

<sup>30</sup> *Id.* at 574.

<sup>31</sup> *In re Grand Jury Subpoena*, 745 F.3d 681, 684 (3<sup>rd</sup> Cir. 1984).

he would make the payment anyway. Later that month, the payment was made to the banker's sister. The bank, in turn, discovered the payment and the FBI became involved in the investigation.<sup>32</sup>

The grand jury served the attorney with a subpoena, and the government moved to enforce, seeking an order directing the attorney to appear and testify before the grand jury. The corporation and corporation president (the client) moved to intervene, and the District Court granted the request. After briefing, the District Court invited the intervenors and the government to submit questions, and the District Court conducted an in camera examination outside of the presence of the parties. Only the attorney's own counsel was present for the in camera review. Following the review, the District Court issued a memorandum and order granting the government's motion to enforce the subpoena and directing the attorney to testify before the grand jury. Based upon a review of the government's ex parte affidavit and the attorney's in camera testimony, the District Court found a reasonable basis to believe that the intervenors (the corporation and the corporation president) intended to commit a crime when the corporate president consulted the attorney, and that they could have used information obtained from the consultation in furtherance of the crime. The District Court declined the intervenors' request to obtain a transcript of the attorney's in camera testimony and the intervenors appealed.<sup>33</sup>

On appeal, the Third Circuit underscored the suitability of in camera review when a District Court is called upon to ascertain the applicability of the crime-fraud exception. The Third Circuit also noted that "a district court can properly be entrusted to consider the due process interests and circumstances in each case, and use its discretion to fashion a proper procedure for in camera examination."<sup>34</sup> The ex parte affidavit, which contained details about the FBI's investigation into the bank and corporation's relationship, and which included the attorney's statement to the FBI about being consulted regarding the project, provided additional support for the in camera examination.<sup>35</sup>

The Third Circuit also emphasized the importance of the relative timing of the client's requisite criminal intent in relation to consultation with counsel, as a factor which a District Court must consider when determining whether the crime-fraud exception applies to attorney-client communications. The client must be "committing or intending to commit a crime or fraud" at the time that the client consults with the attorney.<sup>36</sup> The crime-fraud exception does not, by its terms, apply to a situation where a client consults an attorney about a possible course of action and then subsequently forms the criminal intent to undertake an action.<sup>37</sup> The crime-fraud exception is not applicable where "the client innocently proposes an illegal course of conduct to explore with his counsel what he may or may not do."<sup>38</sup>

That is to say, the exception does not apply where the client forms the intent to engage in criminal or fraudulent activity only after consulting with counsel. It is for the government to demonstrate to the satisfaction of the District Court that the client's criminal intent existed at the time of the attorney-client consultation. The Third Circuit discussed the hypothetical situation where a client who consults with an attorney intends to go as close to the line of illegality as possible while remaining in the realm of legal conduct. The attorney provides advice, explaining what actions would be legal and which actions would be illegal. A year later, the client decides to cross the line and engage in criminal conduct. Does the crime-fraud exception to the privilege apply? The Third Circuit answered no, because the client was not

---

<sup>32</sup> *Id.* at 685.

<sup>33</sup> *Id.* at 686.

<sup>34</sup> *Id.* at 688.

<sup>35</sup> *Id.* at 689-90.

<sup>36</sup> *Id.* at 691, *quoting* *In re Grand Jury*, 705 F.3d 133, 153 (3d Cir. 2012).

<sup>37</sup> *Id.*

<sup>38</sup> *United States v. Doe*, 429 F.3d 450, 454 (3d Cir. 2005).

committing a crime or fraud or intending to commit a crime or fraud at the time of the consultation with counsel.<sup>39</sup>

In the case before the Third Circuit, the court concluded that the District Court did not abuse its discretion in determining that the client intended to commit the crime when he consulted with counsel about making a possible payment. The District Court could infer the client's pre-existing intent to make the payment in part from his statement that he was going to make the payment anyway, after the attorney told him that he should not do so. Furthermore, this evidence helped delineate for the District Court the connection required between the advice sought and the crime or fraud.<sup>40</sup>

An in camera review of subpoenaed grand jury evidence is typically sought by federal prosecutors when the crime-fraud exception is asserted. However, this is not always the case. On occasion, it may be the target of the grand jury or an attorney subject to a grand jury subpoena who requests the district court to review in camera whether particular documents are discoverable, notwithstanding the general application of the crime-fraud exception. An example of this practice is a recent First Circuit decision, *In re Grand Jury Proceedings*.<sup>41</sup> The grand jury investigation in that case arose from a claim in admiralty to issue a warrant of arrest for the physical recovery of a British cargo ship that was sunk by a German U-boat off the coast of Massachusetts in 1942. Appellant, the target of the grand jury investigation, operated a salvage company and sought to raise money from investors to recover the sunken ship and its contents. Evidence developed during the course of the grand jury investigation revealed that appellant falsified documents related to the sunken ship's cargo, thereby creating the misimpression with investors that the sunken ship contained huge quantities of platinum, gold, and possibly industrial diamonds. Documents obtained by the government and recorded conversations monitored by federal agents revealed the scope of the fraud.<sup>42</sup>

Following the execution of a search warrant at the target-appellant's home and the recovery of physical evidence, including computers and electronic devices, the government served grand jury subpoenas on three of appellant's admiralty lawyers. The lawyers asserted the attorney-client privilege and work-product protection. In response, the government filed a motion to compel and a separate motion requesting a determination that the materials seized from the appellant's home were covered by the crime-fraud exception. The government attached a supporting affidavit that summarized the investigation. Appellant filed a motion to intervene, asserting the attorney-client privilege, which was granted. Appellant and one of his three admiralty attorneys subsequently filed an opposition to the motion to compel.<sup>43</sup> Appellant argued that although the government had not requested an in camera review, if the court were "inclined to grant the Motion [to compel], it is hard to imagine the Court doing so before an in camera review has occurred."<sup>44</sup> Appellant's other two admiralty attorneys did not file a motion in response to the motion to compel, and the government represented to the court that they "are asserting the attorney-client privilege with respect to the requested materials but are prepared to produce them upon a requisite court order, and they do not feel the need to be heard in opposition to the motion." They requested the court order to be able to comply with their professional responsibility obligations.<sup>45</sup>

The District Court granted the government's motions to compel and for a judicial determination that the crime-fraud exception applied to evidence seized from appellant's home, finding that the government had proffered prima facie evidence that (1) appellant "participated in a fraud," and (2) "that the admiralty action was connected to the fraud." The District Court did not address appellant's request

---

<sup>39</sup> *In re Grand Jury Subpoena*, 745 F.3d at 691-92.

<sup>40</sup> *Id.* at 692.

<sup>41</sup> *In re Grand Jury Proceedings*, 802 F.3<sup>rd</sup> 57 (1<sup>st</sup> Cir. 2015).

<sup>42</sup> *Id.* at 58-63.

<sup>43</sup> *Id.* at 63-64.

<sup>44</sup> *Id.* at 64.

<sup>45</sup> *Id.*

for in camera review.<sup>46</sup> On appeal, the First Circuit held that the District Court did not abuse its discretion in determining that appellant's communications with his lawyers fell within the ambit of the crime-fraud exception to the attorney-client privilege.<sup>47</sup>

The First Circuit also considered appellant's claim that the grand jury subpoena sought documents that did not further the crime or fraud. The court began its analysis by noting that in camera review can perform two separate functions in the context of the crime-fraud exception. First, it may be used to determine whether the party seeking to invoke the exception has provided sufficient evidence to demonstrate that crime-fraud applies. The second purpose for an in camera review when the crime-fraud exception is invoked, is "to determine whether specific documents evidence communications with attorneys in furtherance of the crime or fraud."<sup>48</sup> The First Circuit surmised that appellant wanted an in camera review in order "to identify documents that remain privileged notwithstanding the existence of the crime-fraud exception because they were not in furtherance of the crime or fraud."<sup>49</sup> The First Circuit concluded that appellant's failure to produce a privilege log or otherwise identify particular documents subject to the privilege to demonstrate the need for an in camera inspection amounted to a waiver and the in camera request was not preserved for appellate review.<sup>50</sup>

A District Court's failure to conduct in camera review of attorney-client documents sought by federal prosecutors may lead to vacatur and a remand.<sup>51</sup> In a matter of first impression, *In re Grand Jury Investigation*, the Ninth Circuit recently held that a District Court's order requiring attorneys to produce all attorney-client documents without in camera review failed to establish that the documents in question were "'sufficiently related to' and 'made in furtherance of the intended, or present, continuing legality.'"<sup>52</sup>

The Ninth Circuit decision resulted from a grand jury investigation of a call center corporation that marketed a surgical device for medical facilities. Allegations had been raised regarding whether the corporation's advertisements adequately advised consumers of potential risks, thereby initiating a Food and Drug Administration (FDA) investigation. A total of three attorneys sent responses to the FDA inquiry on behalf of the corporation. The government alleged that these responses contained false statements which were intended to obstruct the FDA investigation. Relying upon the crime-fraud exception, grand jury subpoenas were issued to the three attorneys to produce "(1) all communications relating to their correspondence to the FDA, including documents and notes showing the information received and identifying the sources of information for the statements and representations made and (2) retainer agreements and billing records identifying the client(s) who retained and paid for their services in communicating with the FDA on the subject matter of the correspondence."<sup>53</sup> The attorneys provided some information in response to the grand jury subpoena but did not fully comply, and the government filed a motion to compel.<sup>54</sup>

Without reviewing any documents in camera, the District Court concluded, based upon independent, non-privileged evidence, that the government had made a prima facie case that the attorneys' services were obtained in furtherance of, and related to, ongoing crimes. The court rejected arguments that in camera review of the privileged documents was necessary to determine whether the

---

<sup>46</sup> *Id.*

<sup>47</sup> *Id.* at 66.

<sup>48</sup> *Id.* at 66-67.

<sup>49</sup> *Id.* at 67.

<sup>50</sup> *Id.* at 68.

<sup>51</sup> *In re Grand Jury Proceedings #5 Empanelled January 28, 2004*, 401 F.3d at 249, 255-56.

<sup>52</sup> *In re Grand Jury Investigation*, 810 F.3d 1110, 1114 (9<sup>th</sup> Cir. 2016), *quoting* *In re Napster, Inc. Copyright Litig.*, 479 F.3d 1078, 1090 (9<sup>th</sup> Cir. 2007).

<sup>53</sup> *Id.* at 1112.

<sup>54</sup> *Id.* at 1112-13.

government made a prima facie case of crime-fraud. The court granted the government's motion to compel production of all "matters identified in the subpoenas."<sup>55</sup>

On appeal, the Ninth Circuit reject appellants' contention that the District Court could not find a prima facie case of crime-fraud without conducting an in camera inspection of the requested documents. "District courts may find a prima facie case of crime-fraud either by examining privileged material in camera or by examining independent, non-privileged evidence."<sup>56</sup> The Ninth Circuit went on to state that the inquiry does not end there. Demonstrating the existence of a prima facie case is only the first step in the inquiry. In a case such as this one, where the government relied on independent, non-privileged evidence to establish reasonable cause to believe that the attorneys were retained to deliver false statements to the FDA, no evidence had been presented to the District Court to establish that the attorney-client communications were "sufficiently related to" and "in furtherance of" the intended, or present, continuing illegality. "Thus far, the litigation has not focused on any individual documents." Rather, "the district court broadly ordered the attorneys to produce everything identified in the government's subpoena, without first examining any specific documents in camera to determine whether they contained communications in furtherance of the asserted crime-fraud."<sup>57</sup> In other words, the District Court's inquiry regarding the applicability of the crime-fraud exception required the District Court to identify the nexus between the attorney-client communication and the intended, present, or continuing crime or fraud. Citing examples from other circuits, the Ninth Circuit vacated and remanded the order compelling production so that the District Court could examine the subpoenaed documents in camera to determine the requisite nexus and proper scope of the production order.<sup>58</sup>

Another example of an overly broad application of the crime-fraud exception which lead to a remand, is a case from the Fifth Circuit, *In re Grand Jury Subpoena*. In a matter of first impression, the Fifth Circuit was asked to address "the scope of the crime-fraud exception to the attorney-client privilege and work product privileges on a record where the grand jury subpoena compelled disclosure of all communications between the attorney and his client, and between the attorney and a third party witness—written, oral or otherwise—rather than discrete communications related to a particular issue or limited to a particular media."<sup>59</sup> The case involved a defendant who was indicted for weapons offenses. The defendant allegedly colluded with his girlfriend, who was a witness to the offense, to obtain legal advice from his then-current counsel that would assist defendant in obstructing criminal proceedings and perpetrating a fraud. In a subsequent investigation, the government served the now-former counsel with a grand jury subpoena and moved to compel the former counsel's compliance as part of the inquiry as to whether the defendant and witness conspired to obstruct justice or commit perjury. The government alleged the crime-fraud exception in support of its motion to compel the attorney's testimony.<sup>60</sup>

In support of the government's motion to compel, an Assistant United States Attorney (AUSA) provided an affidavit urging that the facts supported a strong basis for the District Court to find that the girlfriend-witness and former-defendant-now-appellant had committed perjury and that defendant's former counsel aided and abetted the offense. The AUSA also swore that the facts indicated that the former counsel had refused to participate in the scheme to solicit perjured testimony and to perpetrate a fraud upon the court. Additional documentation submitted by the government in support of the motion to compel included the girlfriend-witness's initial affidavit before an ATF agent; a transcript of the witness's

---

<sup>55</sup> *Id.* at 1113.

<sup>56</sup> *Id.* citing *In re Napster, Inc. Copyright Litigation*, 479 F.3d at 1093; *United States v. Chen*, 99 F.3d 1495, 1503 (9<sup>th</sup> Cir. 1996).

<sup>57</sup> *Id.*

<sup>58</sup> *Id.* at 1114, citing *In re BankAmerica Corp. Securities Litigation*, 270 F.3d at 644; *In re Antitrust Grand Jury*, 805 F.2d 155, 168-69 (6<sup>th</sup> Cir. 1986).

<sup>59</sup> *In re Grand Jury Subpoena*, 419 F.3d 329, 340 (5<sup>th</sup> Cir. 2005).

<sup>60</sup> *Id.* at 333.

testimony before the grand jury; defendant-appellant's letter requesting new counsel; and additional supporting documentation. The District Court conducted an in camera examination of the former counsel and found that the government had met its prima facie case, showing that the crime-fraud exception applied and ordering the former client to comply with the grand jury subpoena.<sup>61</sup>

Appellant moved to quash his former counsel's grand jury subpoena, filed timely notice of appeal, and moved the District Court to stay the execution of the order, pending the appeal. The District Court granted the stay.<sup>62</sup> On appeal, the Fifth Circuit concluded that the District Court was not clearly erroneous in finding that the government had made a sufficient prima facie showing that the crime-fraud exception applied to both the attorney-client and work product privileges. The issue that raised the court's concern was the District Court's overly broad application of crime-fraud. The Fifth Circuit emphasized that the scope of the crime-fraud exception does not extend to all communications made during the course of the attorney-client relationship which, in this case, extended for over nine months. Rather, the crime-fraud exception is limited to those communications and documents in furtherance of the ongoing criminal or fraudulent conduct.<sup>63</sup>

The Fifth Circuit also noted that "because the court's orders compel Former Counsel to appear and order that he cannot assert any attorney-client or work product privilege, no boundary exists as to the extent of his compelled testimony."<sup>64</sup> Hence, the Fifth Circuit determined that the District Court's application of the crime-fraud exception was overly broad and lacking in "the requisite specificity."<sup>65</sup> "[T]he only attorney-client communications and work product materials falling within the scope of the crime-fraud exception are those shown to hold 'some valid relationship' to the prima facie violation such that they 'reasonably<sup>66</sup> related to the fraudulent activity.'" The precise formulation of a test for relatedness is less important, according to the Fifth Circuit, than understanding what the test must accomplish. It is for the District Court when applying the crime-fraud exception to balance the government's immediate concern with obtaining otherwise privileged testimony and documentation against the constitutionally based Sixth Amendment adversarial concerns of the appellant and of the adversarial process.<sup>67</sup>

### **III. The Evidentiary Showing Needed to Support Application of the Crime-Fraud Exception—A Circuit Split as to What is Required**

What threshold showing must federal prosecutors make in order to overcome the attorney-client privilege? There is a Circuit split as to what is required in order to establish sufficient proof to obtain otherwise privileged evidence for introduction into a grand jury proceeding. Therefore, federal prosecutors should review closely case law in their own Circuit.<sup>68</sup> The First Circuit has concluded that "[i]f the party asserting the crime-fraud exception makes . . . [a] reasonable cause showing (also referred

---

<sup>61</sup> *Id.* at 333-34.

<sup>62</sup> *Id.* at 334-35.

<sup>63</sup> *Id.* at 340-43.

<sup>64</sup> *Id.* at 344.

<sup>65</sup> *Id.* at 344-45, *citing* *In re Grand Jury Subpoenas*, 144 F.3d 653, 661 (10<sup>th</sup> Cir. 1998); *In re Vargas*, 723 F.2d 1461, 1467 (10<sup>th</sup> Cir. 1983). *See also* *In re Richard Roe, Inc.*, 68 F.3d 38, 41 (2<sup>d</sup> Cir. 1995); *In re Grand Jury Subpoena Duces Tecum Dated Sept. 15, 1983*, 731 F.2d 1032, 1038 (2<sup>d</sup> Cir. 1984); *In re Sealed Case*, 676 F.2d at 812.

<sup>66</sup> *Id.* at 346, *quoting* *In re Int'l Sys. & Controls Corp. Sec. Litig.*, 693 F.2d at 1235, 1243 (5<sup>th</sup> Cir. 1982).

<sup>67</sup> *Id.* at 347.

<sup>68</sup> *See* *In re Grand Jury*, 705 F.3d at 152-53 (discussing different Circuit measures of proof).

to as a prima facie case), the privilege is forfeited.”<sup>69</sup> The Third<sup>70</sup>, Sixth,<sup>71</sup> and Ninth Circuits<sup>72</sup> have applied similar analyses as the First Circuit, with the Third granting the District Court an especially flexible framework for review of the factual basis to apply the crime-fraud exception.<sup>73</sup>

The Second Circuit has adopted a comparable analysis. In the Second Circuit, the party seeking to invoke the crime-fraud exception must demonstrate that there is a factual basis for a showing of probable cause to believe that a fraud or crime has been committed and that the said communications were in furtherance of the fraud or crime. The proposed factual basis must strike a “prudent person” as constituting “a reasonable basis to suspect” an actual or attempted crime or fraud and communications in furtherance thereof. Once the factual basis is established, it is within the discretion of the District Court whether to engage in an *in camera* review of the evidence. If the District Court elects to conduct the *in camera* review, it is for the District Court to determine whether the facts support application of the crime-fraud exception. The District Court’s factual determinations are governed by the clearly erroneous standard of review.<sup>74</sup>

The Fifth and Seventh Circuits approach the necessary showing for application of the crime-fraud exception somewhat differently. In the Fifth Circuit, the government’s prima facie showing must produce evidence “such as will suffice until contradicted and overcome by other evidence . . . a case which has proceed upon sufficient proof to that stage where it will support [a] finding if evidence to the contrary is disregarded.”<sup>75</sup> Similarly, the Seventh Circuit provides that in order for the government to establish the crime-fraud exception and overcome the attorney-client privilege, the government must “present prima facie evidence that gives color to the charge by showing some foundation in fact.”<sup>76</sup> This evidence allows the District Court to require the party asserting the privilege “to come forward with an explanation for the evidence offered against [the privilege].”<sup>77</sup>

The Fourth, Eleventh, and D.C. Circuits take a third approach, requiring a prima facie showing of evidence that, if believed by the trier of fact, would demonstrate that some violation was ongoing or soon-to-be-committed, and that the attorney-client communications were used in furtherance of the scheme.<sup>78</sup>

---

<sup>69</sup> *In re Grand Jury Proceedings*, 802 F.3d at 66; *In re Grand Jury Proceedings*, 417 F.3d at 22-24 (“‘*Prima facie*’ is among the most rubbery of all legal phrases; it usually means little more than a showing of whatever is required to permit some inferential leap sufficient to reach a particular outcome.”).

<sup>70</sup> *In re Grand Jury #3*, 847 F.3d 157, 165 (3<sup>rd</sup> Cir. 2017) (“reasonable basis to suspect”); *In re Grand Jury Subpoena*, 745 F.3d 681, 689-90 (3<sup>rd</sup> Cir. 2014) (“good faith belief”); *In re Grand Jury*, 705 F.3d at 153 (“reasonable basis to suspect”).

<sup>71</sup> *United States v. Collis*, 128 F.3d 313, 321 (6<sup>th</sup> Cir. 1997) (“prima facie showing”).

<sup>72</sup> *In re Grand Jury Investigation*, 810 F.3d 1110, 1113-14 (9<sup>th</sup> Cir. 2016) (“*prima facie case*”); *In re Grand Jury Proceedings*, 87 F.3d 377, 379-80 (9<sup>th</sup> Cir. 1996) (“prima facie showing”).

<sup>73</sup> *See In re Grand Jury Subpoena*, 745 F.3d at 688 (“We do not want to incentivize circumventing the proper application of the crime-fraud exception. As for the due process implications, we believe that a district court can properly be entrusted to consider the due process interests and circumstances in each case, and use its discretion to fashion a proper procedure for the *in camera* examination.”).

<sup>74</sup> *United States v. Jacobs*, 117 F.3d 82, 87 (2<sup>d</sup> Cir. 1997).

<sup>75</sup> *In re Grand Jury Subpoena*, 419 F.3d 329, 336 (5<sup>th</sup> Cir. 2005), *quoting In re Int’l Sys. & Controls Corp. Sec. Litig.*, 693 F.2d 1235 at 1242. *See United States v. Edwards*, 303 F.3d 606, 618 (5<sup>th</sup> Cir. 2002) (district court’s findings that the crime-fraud exception applies reviewed for clear error only).

<sup>76</sup> *United States v. Boender*, 649 F.3d 650, 655 (7<sup>th</sup> Cir. 2011), *quoting United States v. BDO Seidman, LLP*, 492 F.3d 806, 818 (7<sup>th</sup> Cir. 2007).

<sup>77</sup> *Id.*, *quoting United States v. BDO Seidman, LLP*, 492 F.3d 806, 818 (7<sup>th</sup> Cir. 2007).

<sup>78</sup> *See In re Grand Jury Proceedings #5 Empanelled January 28, 2004*, 401 F.3d at 251, 254 (A district court’s determination that the government made a prima facie showing of crime or fraud should be upheld absent a clear

Finally, in the Eighth Circuit, “a party seeking discovery of privileged communications based upon the crime-fraud exception must make a threshold showing ‘that the legal advice was obtained in furtherance of the fraudulent [or criminal] activity and was closely related to it.’”<sup>79</sup> A moving party does not satisfy the threshold burden merely by alleging that a fraud or crime occurred and asserting that disclosure of any privileged communications may help prove the alleged offense. There must be a specific showing that a particular document or communication was made in furtherance of the client's alleged crime or fraud.<sup>80</sup>

#### **IV. The District Court’s Ex Parte Consideration of the Government’s Motion to Set Aside the Attorney Client Privilege Due to Crime-Fraud: Due Process Challenges**

The target of the federal grand jury or the target’s attorney will, on occasion, raise due process challenges to the ex parte nature of the crime fraud inquiry. Typically, the issue is raised in support of a motion to quash the subpoena compelling the attorney’s testimony and production of documents. The target and the attorney may also seek access to affidavits filed ex parte by the government in support of the government’s showing that the crime-fraud exception to the attorney-client privilege is applicable.

An example of this scenario is *In re Grand Jury Subpoena*, a case of first impression in the Third Circuit. The government in that case was in the midst of an extensive multi-year grand jury investigation, where a subject of the investigation had been represented by retained counsel for over a year. The subject’s attorney was subpoenaed to appear before the grand jury and to produce documents. The attorney moved to quash the subpoena, asserting that his testimony and the production of documents concerning the matter described in the subpoena would disclose privileged attorney-client communications and work product material and would violate the client’s Sixth Amendment right to counsel because the attorney’s testimony would disqualify him from representing the client-subject. The client was granted permission to intervene and raised the same arguments.<sup>81</sup>

The government had earlier provided the attorney with a Schofield affidavit minimally disclosing the purpose of the grand jury investigation. In response to the motion to quash, the government submitted a second Schofield affidavit, this one ex parte, to establish the applicability of the crime-fraud exception to the attorney-client privilege. The ex parte affidavit described the grand jury investigation and included excerpts of testimony and documents obtained during the investigation.<sup>82</sup>

---

showing of abuse of discretion”); *In re Grand Jury Investigation*, 842 F.2d 1223, 1226 (11<sup>th</sup> Cir. 1987); *In re Grand Jury*, 475 F.3d 1299, 1305 (D.C. Cir. 2007).

<sup>79</sup> *In re BankAmerica Corp. Securities Litigation*, 270 F.3d at 641-42, *quoting* *Pritchard-Keang Nam Corp. v. Jaworski*, 751 F.2d 277, 283 (8<sup>th</sup> Cir. 1984). *See In re Grand Jury Subpoenas Duces Tecum*, 798 F.2d 32, 34 (2<sup>d</sup> Cir. 1986).

<sup>80</sup> *Id.* at 642. *See Rabushka ex rel. U.S. v. Crane Co.*, 122 F.3d 559, 566 (8<sup>th</sup> Cir. 1997); *Jacobs*, 117 F.3d at 88.

<sup>81</sup> *In re Grand Jury Subpoena*, 223 F.3d 213, 215 (3<sup>d</sup> Cir. 2000).

<sup>82</sup> *Id.* The *Schofield* affidavit is a Third Circuit practice that originated in the litigation surrounding *In re Grand Jury Proceedings (Schofield I)*, 486 F.2d 85 (3<sup>d</sup> Cir. 1973) and *In re Grand Jury Proceedings (Schofield II)*, 507 F.3d 963 (3<sup>d</sup> Cir.), *cert. denied sub nom. Schofield v. United States*, 421 U.S. 1015 (1975). Concerned with the possibility of restricting judicial review so severely would permit the government to use grand jury subpoenas improperly and realizing that the facts regarding the true purpose of the subpoenas are known only to the government, the *Schofield I* court required the government when seeking enforcement of a grand jury subpoena, to make “some preliminary showing by affidavit that each item is at least relevant to an investigation being conducted by the grand jury and properly within its jurisdiction, and is not sought primarily for another purpose.” *In re Grand Jury Proceedings*, 486 F.2d at 93. For a discussion of *Schofield*, *see In re Grand Jury Proceedings*, 514 F. Supp. 90 (E.D. Pa. 1981).

The District Court held a closed hearing on the motion to quash. Counsel for the subpoenaed attorney and his client argued that without access to the ex parte affidavit, they could not effectively rebut the government's crime-fraud assertions, thereby depriving the client of his due process right to be heard. The District Court rejected these arguments and subsequently issued a memorandum and order denying the motion to quash and directing the attorney to testify before the grand jury. The District Court found that the government's Schofield affidavit adequately described the purpose of the grand jury's investigation and established that the attorney's testimony would be relevant to the investigation. The District Court also concluded that disclosure of the affidavit to the attorney and the target-client would compromise the grand jury investigation. Finally, the Court held that the affidavit provided an adequate basis for invocation of the crime-fraud exception.<sup>83</sup>

On appeal, the Third Circuit reiterated that the grand jury is not an adversarial proceeding. The court noted the District Court's provision that the government make a preliminary showing by affidavit that each item to be subpoenaed was at least relevant to the investigation being conducted and properly within the grand jury's jurisdiction.<sup>84</sup> The Third Circuit determined that the District Court did not abuse its discretion in denying the client-target or his attorney access to this information in order to protect the grand jury's secrecy. The Third Circuit announced that it "join[ed] the ranks of our sister circuits in holding that it is within the district courts' discretion, and not violative of due process, to rely on an ex parte government affidavit to determine that the crime-fraud exception applies and thus compel a target-client's subpoenaed attorney to testify before the grand jury."<sup>85</sup>

Finally, the Third Circuit addressed appellant's Sixth Amendment right to counsel, alluded to in his statement of issues for review but never specifically addressed in argument. A criminal defendant's Sixth Amendment right to counsel does not attach until criminal proceedings have been instituted. No criminal proceeding had yet been initiated, so no right had attached. As for the client-target's argument that requiring his attorney to testify before the grand jury concerning their attorney-client communication would disqualify the attorney as counsel in connection with the investigation and possible future charges, effectively denying the client the right to choose his counsel, the Third Circuit agreed with the District Court that "it is only speculation."<sup>86</sup>

## **V. Mootness Issues Where the Government Presents Crime-Fraud Evidence in a Grand Jury Proceeding Pending Resolution of an Interlocutory Appeal**

Does the appellate court continue to exercise jurisdiction over an appeal of a grand jury evidentiary ruling even after the grand jury has returned both an indictment and a superseding indictment? A recent Third Circuit panel answered in the affirmative, and this decision had consequences for the District Court's application of the crime-fraud exception. *In re Grand Jury # 3* arose from the grand jury investigation of Business A, John Doe, Doe's lawyer, and Doe's business associate for an allegedly fraudulent business scheme. After the government obtained access to an email that Doe claimed was privileged, the government asked the District Court for permission to introduce the email to the grand

---

<sup>83</sup> *In re Grand Jury Subpoena*, 223 F.3d at 215.

<sup>84</sup> *Id.* at 216, *citing* *In re Grand Jury Empaneling of Special Grand Jury*, 171 F.3d 826, 836 (3d Cir. 1999) (witnesses subpoenaed by the grand jury refused to testify against their rabbi father on religious grounds; government opposed the motion to quash the subpoenas; on appeal, the Third Circuit held that the district court did not abuse its discretion in refusing to disclose the government's ex parte affidavit).

<sup>85</sup> *Id.* at 219, *citing* *In re Grand Jury Subpoena as to C97-216*, 187 F.3d 996 (8th Cir. 1999); *In re Grand Jury Proceedings*, 867 F.2d 539, 540-41 (9th Cir. 1989); *In re Grand Jury Proceedings, Thursday Special Grand Jury* Sept. Term, 1991, 33 F.3d at 353; *In re John Doe, Inc.*, 13 F.3d 633 (2d Cir. 1994).

<sup>86</sup> *Id.* at 219-20.

jury. The District Court concluded that although the email was privileged, the crime-fraud exception applied. Doe filed an interlocutory appeal, requesting the Third Circuit to reverse the District Court's order. While the appeal was pending, the grand jury viewed the email and subsequently returned an indictment against Doe, Doe's lawyer, and Doe's business associate for conspiracy to violate the Racketeer Influenced and Corrupt Organizations Act (RICO). Thereafter, the grand jury was dismissed and a new grand jury empaneled. It too viewed the disputed email and returned a superseding indictment which contained revisions to the previous charges.<sup>87</sup>

The first question for the Third Circuit focused on whether the appeal was moot since the first grand jury had returned an indictment and a succeeding grand jury had returned a superseding indictment. Relying on Third Circuit precedent, the court concluded that because the grand jury investigation was continuing, the court retained jurisdiction and could resolve the controversy.<sup>88</sup>

Having concluded that it had jurisdiction, the Third Circuit moved on to the question of whether the crime-fraud exception applied to the attorney email since, without the exception, the government had no basis for introducing the email to the grand jury. Relying upon the Third Circuit's well-established two-prong test, the Third Circuit had no difficulty concluding that the government satisfied the first prong, that there was a reasonable basis for believing that Doe had committed fraud: the government produced a tape recording of Doe bragging about defrauding the class action victim-plaintiffs. The reasonable basis to believe or suspect the existence of the second prong of the test—that the attorney work product was used in furtherance of the alleged crime or fraud—was far less compelling. Here, the only purported act in furtherance of the alleged crime or fraud identified by the District Court was Doe forwarding his attorney's email to the accountant. There was no evidence to support the inference that Doe intended this act to further the crime or fraud. Specifically, there was no evidence that Doe amended his tax returns or planned to amend the tax returns after he forwarded the email. "There is no indication he had ever decided to amend the returns, and before the plan could proceed further the lawyer told the accountant to hold off. Thus Doe at most thought about using his lawyer's work product in furtherance of a fraud, but he never actually did so."<sup>89</sup> The Third Circuit, therefore reversed the District Court's finding regarding application of crime-fraud to the attorney work product.

What of the superseding indictment returned by a grand jury that had reviewed the attorney's privileged email? The Third Circuit reasoned that if Doe were convicted, "none of this should suggest that . . . he should automatically get a new trial because the Government used the protected work product. This is because the Government could avoid a retrial by showing that the error was harmless." The Third Circuit expressed no opinion on the question of whether providing the email to the grand jury constituted harmless error.<sup>90</sup>

## **VI. When the Crime-Fraud Exception Applies—What is the Scope of Attorney Work Product Available to the Grand Jury**

### **A. The Attorney Work Product Doctrine**

An important issue for federal prosecutors seeking to pierce the attorney-client privilege by demonstrating that the crime-fraud exception applies, is the issue of whether attorney work product is also

---

<sup>87</sup> *In re Grand Jury Matter #3*, 847 F.3d at 160.

<sup>88</sup> *Id.* at 162-64, *citing* *In re Search of Elec. Commc'ns in the Account of In re Search of Elec. Commc'ns in the Account of chakafattah gmail.com at Internet Serv. Provider Google, Inc.*, 802 F.3d 516, 521 n. 2 (3d Cir. 2015); *In re Grand Jury Proceedings*, 632 F.2d 1033, 1040 (3d Cir. 1980).

<sup>89</sup> *Id.* at 166.

<sup>90</sup> *Id.* at 167.

protected by privilege. Ordinarily, the work-product doctrine protects from discovery materials prepared or collected by counsel in the course of preparation for possible litigation.<sup>91</sup> The burden of proving applicability of the privilege rests upon the party asserting the privilege. Both the attorney and a client, to the extent that the client may be affected, can assert the privilege.<sup>92</sup> As noted above, a finding of crime-fraud overcomes the work product privilege in much the same way that crime-fraud overcomes the attorney-client privilege: where there is a reasonable basis to believe that the privilege holder was committing or intended to commit a crime or fraud and that the attorney work product was in furtherance of the alleged crime or fraud.<sup>93</sup>

## **B. Attorney Work Product: Preparation for Possible Litigation, and the Scope of the Work Product Privilege**

Several courts have concluded that communications between an attorney and client do not qualify for work product protection unless they are made “in the course of preparation for possible litigation.”<sup>94</sup> These courts have stated that work product prepared in the course of business is not protected from discovery, and an attorney’s recollections and research are also not protected when they are created outside of the context of preparation for possible litigation. However, it is worth noting that “preparation for possible litigation” is typically construed broadly.<sup>95</sup>

Other courts have analyzed the work product doctrine without reference to whether materials prepared by attorneys for a client were in preparation for possible litigation. An excellent example of this work product doctrine analysis and the impact of crime-fraud is a case out of the Fifth Circuit. *In re Grand Jury Subpoenas* involved a lawyer and a law firm that provided advice to a client regarding the tax implications of a series of off-shore trusts. According to the government, neither the lawyer nor the law firm in question were targets of the grand jury, and both were misled by the client as to the actual control and uses of the trusts. The Fifth Circuit case emerged from a long-term grand jury investigation of a complex foreign trust scheme conceived by the appellants, who created twenty-five trusts and forty-eight subsidiary corporations in the Isle of Man and the Cayman Islands to promote securities and tax fraud. The grand jury investigation revealed that the massive fraud schemes were facilitated by several different lawyers and law firms.<sup>96</sup>

The Fifth Circuit case originated from a grand jury subpoena that was issued to the lawyer and law firm in question, who resisted on grounds of the attorney-client and work product privilege. The government responded by arguing before the District Court that it was relying on the crime-fraud exception to rebut the privilege. The law firm, in turn, filed a privilege log and an opposition motion, and the District Court ordered an in camera review of the documents claimed to be privileged. The law firm surrendered the documents but filed a motion for a partial reconsideration, contending that the court should not review some of the documents—the “core work product” documents—until the court made a

---

<sup>91</sup> *Hickman v. Taylor*, 329 U.S. 495, 505 (1947).

<sup>92</sup> *In re Green Grand Jury Proceedings*, 492 F.3d 976, 981 (8<sup>th</sup> Cir. 2007) (an attorney who did not knowingly participate in his client’s crime or fraud may assert the work product privilege as to his opinion work product). *See also In re Grand Jury Proceedings #5 Empanelled January 28, 2004*, 401 F.3d at 250 (“Because the work product privilege protects not just the attorney-client relationship but the interests of attorneys to their own work product”, both the attorney and the client hold the privilege.).

<sup>93</sup> *In re Grand Jury Subpoena*, 745 F.3d at 693-94; *In re Grand Jury*, 705 F.3d at 153. *See also*, *In re Grand Jury Subpoena*, 419 F.3d at 335.

<sup>94</sup> *In re Grand Jury Investigation*, 599 F.2d 1224, 1228 (3d Cir. 1979) (quoting *Hickman*, 329 U.S. at 505). *See also In re Grand Jury*, 870 F.3d 312, 2017 WL 3567824 (4<sup>th</sup> Cir. 2017) and FED.R.CIV.P. 26(b)(3).

<sup>95</sup> *In re Grand Jury Subpoena*, 745 F.3d at 694, *citing Holmes v. Pension Plan of Bethlehem Steel Corp.*, 213 F.3d 124, 138 (3d Cir. 2000).

<sup>96</sup> *In re Grand Jury Subpoenas*, 561 F.3d 408, 409-10 (5th Cir. 2009).

threshold determination that the government had produced evidence justifying the review. Appellants intervened, also objecting to the government’s motions.<sup>97</sup>

The District Court concluded that the crime-fraud exception applied to all of the law firm’s communications regarding the foreign trusts and ordered these documents disclosed to the government. Some of the documents reviewed in camera did not relate to the trusts, and these were not disclosed. Other documents were redacted of unrelated material. The District Court agreed that three documents included “opinion work product,” but nonetheless ordered them disclosed because the government demonstrated a serious need for the documents. Disclosure of the three documents was conditioned on a government stipulation that it would use “the documents and any evidence derived from the documents only in connection with establishing the mental state of Intervenor with respect to any statements to or filings with the government . . . on or after July 1, 1997.”<sup>98</sup>

On appeal, the Fifth Circuit began its analysis by noting that work product protections, unlike the attorney-client privilege, are held by the attorneys as well as the client. The party intending crime or fraud cannot invoke the work product doctrine. However, if the other party does not intend crime or fraud, that other party can invoke it. Where there was no evidence of criminal or fraudulent intent by the lawyer or the law firm, both could invoke the work product privilege for relevant documents, as they did before the District Court. On appeal, however, neither the lawyer nor the law firm invoked the privilege. Only the appellants invoked.<sup>99</sup>

The Fifth Circuit affirmed the judgment of the District Court that appellants’ right to invoke the privilege was forfeited by a showing, sufficient to overcome the privilege, of their alleged intention of soliciting legal advice to further their criminal activities. Hence, the work product privilege was not available to them.<sup>100</sup> The Fifth Circuit also rejected appellants’ argument that the District Court order of production was overbroad. Specifically, appellants claimed that the crime-fraud exception could not apply, as a matter of law, to documents that contained legal advice concerning past conduct and could only apply to documents pertaining to prospective conduct. They also urged that the District Court’s order was overbroad because the court failed to conduct a document-by-document analysis.<sup>101</sup>

The Fifth Circuit noted that “the conduct in this case was not past in a relevant way at the time the advice was sought and given. To the contrary, the government alleges—and has produced ample evidence to support its allegations—that the criminal actions were ongoing. And occasional backward looks were only part of a forward looking scheme that drew on these validations.”<sup>102</sup> Finally, a document-by-document analysis was not necessary because all communications at issue appeared to bear a reasonable relation to the furtherance of ongoing crime.<sup>103</sup>

In the Fifth Circuit case, three documents described as opinion work product were disclosed to the government, subject to special qualifying conditions. Indeed, opinion work product creates special challenges when courts engage in a crime-fraud analysis, and the courts are not consistent in their approach. It is important to remember that the attorney-client privilege encompasses both “fact” work product and “opinion” work product. Fact work product consists of documents prepared by an attorney

---

<sup>97</sup> *Id.* at 410.

<sup>98</sup> *Id.* at 410-11.

<sup>99</sup> *Id.* at 411.

<sup>100</sup> *Id.* at 412. The Fifth Circuit also rejected any suggestion that *Perlman v. United States*, 247 U.S. 7 (1918) applied, which allows for client intervention in cases where attorneys are compelled to produce protected documents, because this right is subject to the crime-fraud exception.

<sup>101</sup> *Id.*

<sup>102</sup> *Id.*

<sup>103</sup> *Id.* at 412-13.

that do not contain the attorney’s impressions. Opinion work product does contain the fruits of the attorney’s mental processes and is more scrupulously protected.<sup>104</sup>

### C. Fact Work Product and Attorney Opinion Work Product

A recent case from the Fourth Circuit demonstrates issues surrounding opinion work product and application of the crime-fraud exception. *In re Grand Jury Subpoena* arose after the conviction of a criminal defendant at trial, where one of the exhibits introduced into evidence, the photocopy of a document, appeared to be a forgery. Upon request, defense counsel subsequently provided the government a better quality copy of the exhibit, which appeared to confirm the government’s suspicions and raised new questions. Defense counsel and her investigator (the Defense Team) declined the government’s request for interviews and objected to the grand jury issued subpoenas compelling their testimony. The Defense Team moved to quash, arguing protected work product. The government, in turn, clarified that it intended to ask three questions: “(1) Who gave you the fraudulent documents?; (2) How did they give them to you, specifically?; and (3) What did [a specific party under investigation] tell you?” The District Court held that the testimony sought constituted fact work product, but that the government had made a prima facie showing that the crime-fraud exception applied and that the questions could be asked in the grand jury. The District Court denied the motion to quash, and an appeal followed.<sup>105</sup>

The Fourth Circuit first considered the scope of the privilege. Because the work-product privilege protects both the attorney-client relationship and the interests of attorneys in their own work-product, the attorney and the client both hold the privilege. Fact work product is a “transaction of the factual events involved” and may be obtained upon a showing of substantial need and the inability to secure substantially equivalent materials without undue hardship.<sup>106</sup> Opinion work product, however, contains “the actual thoughts and impressions of the attorney,” “is more scrupulously protected,” and can be discovered only in rare circumstances. Indeed, a party seeking to compel production of opinion work-product must show that the attorney had knowledge of or participated in the client’s crime or fraud.<sup>107</sup>

In its analysis, the Fourth Circuit determined that the government’s first two questions targeted fact work product, which the government sought pursuant to the crime-fraud exception. Because the government had made the requisite prima facie showing—(1) that the client was engaged in or planning a criminal or fraudulent scheme when he sought the advice of counsel to further the scheme, and (2) that the information sought bore a close relationship to the client’s existing or future scheme to commit a crime or fraud—the District Court did not abuse its discretion in finding that the government demonstrated crime-fraud. The government’s third proposed question, however, asked for opinion work product and therefore required a different analysis.<sup>108</sup>

In order to overcome the opinion work product privilege, the government was required to make a prima facie showing that the attorney was aware of, or a knowing participant in, the criminal conduct.<sup>109</sup> Because the government did not allege that the Defense Team was aware of the putative crime or fraud, the government could not rely on the crime-fraud exception to compel the Defense Team to answer the third question, which implicated the protected opinion work product. Therefore, the Fourth Circuit reversed the District Court’s order regarding question number three.<sup>110</sup>

---

<sup>104</sup> *In re Grand Jury Proceedings #5 Empanelled January 28, 2004*, 401 F.3d at 250. (Citations omitted).

<sup>105</sup> *In re Grand Jury Subpoena*, 870 F.3d at 315.

<sup>106</sup> *Id.* at 316, *quoting* *In re Grand Jury Proceedings*, 102 F.3d 748, 750 (4th Cir. 1996).

<sup>107</sup> *Id.*, *quoting* *In re Grand Jury Proceedings*, 102 F.3d at 750.

<sup>108</sup> *Id.* at 316-17.

<sup>109</sup> *Id.* at 316 *citing* *In re Grand Jury Proceedings #5 Empanelled January 28, 2004*, 401 F.3d at 254.

<sup>110</sup> *Id.* at 319.

The Eighth Circuit has adopted a similar analysis to the Fourth with regard to opinion and non-opinion attorney work product. *In re Grand Jury Proceedings, G.S., F.S.* involved a grand jury proceeding with allegations of bankruptcy fraud. The government sought to compel the clients' attorney to produce documents and to testify. The government alleged crime-fraud, and the attorney resisted the government's discovery of his work product, claiming that it was opinion and non-opinion work product. In this case, the government alleged that the attorney was himself complicit in his client's unlawful activity and that all of the work product sought pursuant to the grand jury subpoena was discoverable. On appeal, the Eighth Circuit concluded that the District Court did not abuse its discretion and that there was a reasonable likelihood that the attorney "knew or was willfully blind to the fact that his clients were entering sham transactions."<sup>111</sup>

The analysis is somewhat different when there is no indication that the attorney engaged in the crime or fraud. An Eighth Circuit case that focuses on the application of the crime-fraud exception to an attorney's opinion work product where no attorney misconduct is alleged, is *In re Green Grand Jury Proceedings*. The case arose from an investigation of a client, who was the target of a grand jury investigation alleging improperly received payments. In responding to these allegations, the client retained counsel and provided his attorney with an alternate, non-criminal explanation for the payments. The attorney relied upon his client's representations in preparing his legal advice and in drafting documents that memorialized what the client said had occurred. The government's investigation indicated that the client knowingly lied to his attorney and provided a false back-story to explain payments that the client improperly received.<sup>112</sup>

The grand jury issued subpoenas to the client's attorney and the attorney's law firm, seeking documents and the attorney's testimony. In response, the law firm produced a privilege log, identifying 1,604 documents. The firm claimed that the documents were protected under the attorney-client or work product privilege, and the attorney declined to answer the grand jury's questions. The government, in turn, moved to compel production of the documents and the attorney's testimony.<sup>113</sup>

The District Court reviewed 179 documents in camera and concluded that under the crime-fraud exception, the client could not assert the attorney-client or work product privileges because the government had presented a prima facie case that the client used his attorney's counsel in furtherance of a fraud. Like the recent Fourth Circuit case discussed above, the District Court concluded that because there was no evidence that the attorney had known of the client's fraud, there was nothing to preclude the attorney from asserting his own work product privilege as to any opinion work product that might be contained therein. The court permitted the attorney to decline to answer the grand jury's questions, except for questions pertaining to the origins of the documents. Answers to "questions relating to the origins of documents" do not constitute recollections on par with notes and are therefore fact work product." Only the attorney's opinion work product was protected, not the fact work product. The court also determined that the remainder of the documents it reviewed were not discoverable under the crime-fraud exception because they were not generated in furtherance of any fraud.<sup>114</sup>

The government contested the redactions and the restrictions on the attorney's grand jury testimony. The client also appealed the portion of the district court's order requiring production of the thirty-six documents and the attorney's limited testimony.<sup>115</sup>

On appeal, the Eighth Circuit emphasized that the attorney's independent assertion of the work product privilege is separate and distinct from the client's work product privilege because "the attorney's

---

<sup>111</sup> *In re Grand Jury Proceedings, G.S., F.S.*, 609 F.3d 909, 915 (8<sup>th</sup> Cir. 2010).

<sup>112</sup> *In re Green Grand Jury Proceedings*, 492 F.3d at 978.

<sup>113</sup> *Id.* at 978-79.

<sup>114</sup> *Id.* at 979.

<sup>115</sup> *Id.*

privilege is based on the attorney's interest in protecting his opinions and thought processes from disclosure. This is a protection that benefits all of the attorney's clients because it accords the attorney a measure of privacy within which he can candidly compose his thoughts."<sup>116</sup> Like the Fourth Circuit in the case above, the Eighth Circuit distinguished between ordinary work product—"raw factual information—and opinion work product, which encompasses the attorney's mental impressions, conclusions, opinions or legal theories."<sup>117</sup> In affirming the district court, the Eighth Circuit rejected the government's argument that the attorney's notes and recollections about conversations with the client were discoverable. "Notes and memoranda of an attorney, or an attorney's agent, from a witness interview are opinion work product entitled to almost absolute immunity."<sup>118</sup>

In situations where the government does not allege that the attorney engaged in crime or fraud, can the grand jury ever obtain access to work product that may include an attorney's opinion? As noted above, the Fifth Circuit allowed very narrow access to limited opinion work product—three documents—on grounds that the government had demonstrated "a serious need" for the documents, conditional upon a government stipulation that "it will use the documents and any evidence derived from the documents only in connection with establishing the mental state of Intervenors with respect to any statements to or filings with the government...on or after July 1, 1997 . . ."<sup>119</sup> Judge Niemeyer's dissent in the Fourth Circuit in the *In re Grand Jury Subpoena* case lends support for the proposition that there are circumstances where "necessity and justice require their production".<sup>120</sup> Judge Niemeyer also noted previous Fourth Circuit decisions that afford opinion work product scrupulous but not absolute protection.<sup>121</sup>

When confronted with a challenge by counsel that subpoenaed information is opinion work product and therefore not subject to discovery, prosecutors should be prepared to support the grand jury's request, where possible, by specifying precisely what information and why the information is needed. As Judge Niemeyer noted, "Hickman and its progeny favor disclosure of what are historical facts." When the grand jury is seeking an attorney's testimony about what a witness said about a particular document, that request does not implicate the attorney's impressions about the witness's statement or require the attorney to evaluate the witness's statement and, indeed, the attorney can be expressly instructed to omit any impressions in the attorney's responses.<sup>122</sup>

## D. Opinion Work Product by Any Other Name

Finally, there is the broad approach to the admissibility of attorney-client work product adopted by the Third Circuit in the case of *In re Grand Jury Investigation*. In this case, the district court's determination that evidence of crime-fraud supported the grand jury's request for the attorney's notes and testimony about conversations with a client was affirmed without any discussion of the distinction between fact work product and opinion work product. The case involved the in-house lawyer's advice to corporate employees about grand jury subpoena compliance. The in-house lawyer contacted employees who might have documents responsive to the grand jury's inquiry. The government was not satisfied with the corporation's initial response and followed up with a second subpoena to the organization. The following day, the government informed the organization that it intended to have FBI and IRS technicians scan the organization's computers to recover deleted emails and other electronic records. The in-house attorney contacted Jane Doe, the organization's executive director, to discuss these matters. Subsequently,

---

<sup>116</sup> *Id.* at 980.

<sup>117</sup> *Id.*, citing *Baker v. Gen. Motors Corp.*, 209 F.3d 1051, 1054 (8th Cir. 2000).

<sup>118</sup> *Id.* at 981-82, quoting *Baker*, 209 F.3d at 1054.

<sup>119</sup> *In re Grand Jury Subpoenas*, 561 F.3d at 411.

<sup>120</sup> *In re Grand Jury Subpoena*, 870 F.3d at 321, citing *Hickman*, 329 U.S. at 509, 511-12.

<sup>121</sup> *Id.*, citing *In re Grand Jury Proceedings #5 Empanelled January 28, 2004*, 401 F.3d at 252; *In re Grand Jury Proceedings*, 102 F.3d at 750.

<sup>122</sup> *Id.* at 322.

FBI technicians who took mirror images of the organization’s hard drives, uncovered evidence suggesting that employees of the organization, including Jane Doe, had attempted to delete emails. The government sought to compel production of the in-house lawyer’s notes regarding his conversation with Jane Doe about the subpoena, and to obtain the attorney’s testimony about the substance of his conversation with her. The District Court ordered the attorney to produce his notes and to testify about his conversations with Jane Doe, once the government demonstrated the applicability of the crime-fraud exception. The District Court denied a stay pending the appeal, and the Third Circuit also denied a stay. Notably, the issue of heightened protection for opinion work product was evidently not raised by the parties in either the District Court or the Third Circuit. However, the breath of the required attorney disclosure implicates what is typically considered opinion work product.<sup>123</sup>

Several points from the Third Circuit opinion underscore how broadly the court construed the scope of the grand jury’s inquiry once the application of the crime-fraud exception was demonstrated to the satisfaction of the District Court. Notably, Jane Doe did not initiate the communication with in-house counsel. Instead, she received the unsolicited legal advice on how to satisfy the organization’s legal obligations regarding the grand jury investigation from in-house counsel. The Third Circuit noted that Jane Doe’s personal lawyer and in-house counsel entered into a joint defense agreement, so the attorney-client privilege between Doe and in-house counsel was applicable. The court also cited Supreme Court precedent that communications between corporate counsel and corporate employees are covered by the privilege.<sup>124</sup>

The Third Circuit rejected Doe’s contention that the crime-fraud exception was inapplicable to her because she did not initiate the communication or solicit the advice of in-house counsel. “There would be no reason to limit the applicability of the crime-fraud exception to client-initiated contact, as the exception’s purpose is to further frank and open exchanges between the client and his or her attorney, whether newly retained for purposes of the investigation or otherwise.”<sup>125</sup>

The government in this case met its burden of showing that the crime-fraud exception applied with a prima facie showing to the District Court, which included an ex parte affidavit. The Third Circuit conceded that the secrecy “hampered” the explanation of its affirmance of the District Court finding of crime-fraud, but agreed with the District Court that “at the time of Jane Doe’s . . . conversation with Attorney, Jane Doe was committing the crime of obstruction of justice.”<sup>126</sup> Moreover, “[o]ne may infer . . . that the obstruction of justice that the Government is investigating is the deletion of potentially relevant email files with knowledge of their relevance to the grand jury’s investigation.”<sup>127</sup>

In acknowledging the uniqueness of the fact pattern before it, the Third Circuit averred that “there are no [court] opinions of which we are aware that apply the crime-fraud exception in precisely these circumstances. However, we see no reason why it does not apply.” Relying upon the statements and applied analogies used by the Assistant U.S. Attorney during oral argument, the court inferred “that in the course of communications between Jane Doe and Attorney, Attorney advised Jane Doe of the contents of the most recent subpoena and of the Government’s interest in retrieving from Organization’s computers emails to or from certain persons, including Jane Doe . . .” The court emphasized that there was no evidence of misconduct or malfeasance on the part of counsel.<sup>128</sup>

The Third Circuit concluded that the District Court properly tailored its order regarding the attorney’s testimony and production of the attorney’s notes concerning his conversation with Jane Doe

---

<sup>123</sup> In re Grand Jury Investigation, 445 F.3d at 268-70.

<sup>124</sup> *Id.* at 273, *citing* Upjohn Co., 449 U.S. at 397.

<sup>125</sup> *Id.* at 274.

<sup>126</sup> *Id.* at 275.

<sup>127</sup> *Id.* at 277.

<sup>128</sup> *Id.* at 278-79.

regarding the organization's compliance with two grand jury subpoenas and a letter indicating that the government wished to have the FBI and IRS experts scan the organization's computers to recover stored information, including deleted email files. The District Court's order covered only subjects implicated by the crime-fraud exception.<sup>129</sup>

Prosecutors who seek to use the crime-fraud exception to obtain opinion work product information that is usually privileged must be prepared to make a compelling argument establishing not only the prima facie case for production but also the compelling need for the evidence and the ultimate purpose of the grand jury proceeding, which is the pursuit of justice. For the Third Circuit in *In re Grand Jury Investigation*, for the Fifth Circuit in *In re Grand Jury Subpoenas*, and for Judge Niemeyer in his dissent in *In re Grand Jury*, the question of what attorney work product and attorney-client privilege communications may be abridged as a result of crime-fraud comes down to this: "[w]e cannot lose sight of the ultimate fact that the attorney-client privilege is designed to promote the fair administration of justice."<sup>130</sup> A client's criminal misuse of an attorney's legal advice clearly frustrates this goal.<sup>131</sup>

## VII. Conclusion

The crime-fraud exception to the attorney-client and work product privileges offers an important potential tool for prosecutors who confront criminal conduct, fraud, or obstruction of justice in the course of an investigation. Effective use of this tool requires compelling evidence that the client used or attempted to use the attorney-client relationship to commit or facilitate crime or fraud. Because the issuance of a grand jury subpoena to an attorney for information relating to the attorney's representation is so consequential, the Department of Justice exercises close control over the process. As a general rule, these subpoenas can only be issued upon authorization of the Assistant Attorney General or Deputy Assistant Attorney General for the Criminal Division. Prosecutors should also consult with their supervisors and the Office of Enforcement Operations.<sup>132</sup>

Finally, effective use of the crime-fraud exception ensures that the federal grand jury is able to obtain essential evidence in support of its mission to secure justice.

### ABOUT THE AUTHOR

**Gretchen C. F. Shappert** is the United States Attorney for the Virgin Islands, and the former Assistant Director for the Indian, Violent and Cyber Crime Staff at the Executive Office for United States Attorneys. Ms. Shappert served as the U.S. Attorney for the Western District of North Carolina from 2004 to 2009. She was also an Assistant U.S. Attorney from 1990 to 2004 and specialized in violent crime and outlaw motorcycle gang prosecutions.

---

<sup>129</sup> *Id.* at 268-69, 280.

<sup>130</sup> *Id.* at 279-80, *citing* *In re Grand Jury Proceedings*, 604 F.2d 798, 802 (3d Cir. 1979).

<sup>131</sup> *Id.* at 280.

<sup>132</sup> UNITED STATE ATTORNEYS' MANUAL (USAM) § 9-13.410; Federal Grand Jury Practice 7.15, 10.2 and 10.19.

# Investigating and Prosecuting Law Enforcement Sexual Misconduct Cases

*Fara Gold*  
*Special Litigation Counsel*  
*Criminal Section*  
*Civil Rights Division*

## I. Introduction

Those who commit crimes involving sexual misconduct exploit the disparate power dynamic between victim and offender, be it teacher and student, producer and actor, coach and athlete, or law enforcement officer and arrestee, probationer, or inmate. By wielding weapons of authority, in the many forms that may take, the perpetrator leaves the victim with little choice but to submit to his actions and stay quiet in the aftermath, fearing that no one will believe her and everyone will blame her.<sup>1</sup> This is especially true in the law enforcement context, where victims are usually in the custody of their offender, have a history of criminal activity, and whose status in life lowers their credibility in the eyes of those that might judge them. After all, who is going to believe a victim with such a background when it is a criminal's word, alleged or otherwise, against an officer, who has a badge and a gun, and who has sworn to uphold the Constitution? In short, such an individual is the perfect victim against whom to commit a crime and get away with it. Investigators and prosecutors therefore have to take care not to immediately discount the account of such victims without further investigation.

To be sure, most law enforcement officers serve their communities honorably. However, for those that do not, the federal government has jurisdiction to prosecute law enforcement officers who commit sexual misconduct under 18 U.S.C. § 242,<sup>2</sup> the statute more commonly used to prosecute law enforcement officers who use unreasonable or excessive force. Section 242 makes it a federal crime for those acting under color of law to willfully deprive an individual of his or her Constitutional or federally protected rights.<sup>3</sup> As described in more detail below, law enforcement officers who engage in nonconsensual sexual contact with individuals in their care or custody or under their authority, for the most part, deprive those individuals of liberty without due process of law in violation of the Fourteenth Amendment,<sup>4</sup> which includes the right to bodily integrity.<sup>5</sup> Depending on the circumstances, these acts may also violate a person's right not to be subjected to "unreasonable searches and seizures,"<sup>6</sup> the right

---

<sup>1</sup> For the sake of consistency and clarity, the pronouns "he" and "him" will be used to refer to perpetrators, and the pronouns "she" and "her" will be used to refer to victim, with the understanding that males can also be victims of crimes of sexual violence, and likewise, females can perpetrate such crimes.

<sup>2</sup> 18 U.S.C. § 242.

<sup>3</sup> *Id.*

<sup>4</sup> U.S. CONST. AMEND. XIV § 1.

<sup>5</sup> See *Doe v. Taylor Indep. Sch. Dist.*, 15 F.3d 443, 451 (5th Cir. 1994) (en banc) (Individuals have a right to be free from sexual assaults committed under color of law just as they have a right to be free from other unreasonable physical assaults); citing *Shillingford v. Holmes*, 634 F.2d 263, 265 (5th Cir.1981) ("[t]he right to be free of state-occasioned damage to a person's bodily integrity" is protected by the Fourteenth Amendment's guarantee of substantive due process).

<sup>6</sup> U.S. CONST. AMEND. IV.

not be subjected to “cruel and unusual punishment,”<sup>7</sup> and the right to privacy.<sup>8</sup> Section 242 covers, among others, police officers, probation officers, corrections officers and other employees of jails and prisons, judges, and other federal, state, and local law enforcement and public officials. Prosecutable acts of sexual misconduct include sexual assault without consent, sexual contact procured by force, threat of force or coercion, and unwanted or gratuitous sexual contact such as touching or groping. There are also instances where gratuitous strip searches, taking of nude photographs, staring, leering, and ogling may be prosecutable. The federal government can also prosecute perpetrators for obstruction of justice, e.g., attempting to prevent the victim from reporting sexual misconduct, lying to federal officials during the course of a federal investigation into the sexual misconduct, and writing a false police report to cover up sexual misconduct.

Because victims are often in the custody or under the authority of their perpetrators, it is not uncommon for them to feel like they cannot report the police to the police. Yet, they often disclose to family, friends, clergy, hospital staff, legal aid groups, tribal leaders, national and local civil rights organizations, counselors, or criminal and civil rights attorneys. These disclosure or “outcry” witnesses are largely unaware of the federal government’s jurisdiction. The Criminal Section of the Civil Rights Division (Criminal Section), which has primary jurisdiction over Section 242 violations, has been working to decrease barriers to reporting by “spreading the word” to the aforementioned stakeholders that the federal government has the ability to hold these offenders accountable, and is thereby able to vindicate the interests of the victims and the communities in which these law enforcement officers serve.

By actively investigating and charging meritorious cases more often, federal prosecutors can increase awareness of our jurisdiction, one case at a time, so that reporting instances of law enforcement sexual misconduct to federal authorities becomes an apparent and realistic option. The underreporting of these crimes is not because they are not happening, but rather because in addition to the general reluctance to report sex crimes, victims of law enforcement sex crimes, in particular, do not know where or how to report. This article will address the steps prosecutors and investigators should take upon learning of a law enforcement sexual misconduct allegation. This article will also look at the statutory nuances of Section 242 in the sexual misconduct context, and the evidentiary hurdles and investigatory challenges associated with effectively prosecuting a sexual misconduct case, where the offender is in law enforcement and the victim lacks credibility by virtue of her status as an arrestee, an inmate, or a probationer. To overcome these hurdles and develop a strong case, there must be an intense focus on developing credible evidence to both corroborate the victim’s account and discredit the anticipated defense of the offender.

## **II. Proving the Elements: 18 U.S.C. § 242**

To establish a violation of Section 242, the government must prove the following elements beyond a reasonable doubt:<sup>9</sup> (1) the defendant must have been acting under color of law; (2) the defendant must have deprived the victim of a right protected or secured by the Constitution or the laws of the United States; and (3) the defendant must have acted willfully.<sup>10</sup> To establish a felony violation of Section 242, the government must prove at least one additional element: (4) either: (a) that the act resulted in bodily

---

<sup>7</sup> U.S. CONST. AMEND. VIII.

<sup>8</sup> *See* *Roe v. Wade*, 410 U.S. 113, 153 (1983) (right to privacy in Fourteenth Amendment’s “concept of personal liberty and restriction upon state action”); *Terry v. Ohio*, 392 U.S. 1 (1968) (freedom from unreasonable governmental intrusion under Fourteenth Amendment); *Griswold v. Connecticut*, 381 U.S. 479, 484, (1965) (recognizing “zones of privacy” found in the First, Third, Fourth, Fifth and Ninth Amendments, but no general right to privacy).

<sup>9</sup> For a comprehensive legal discussion of Section 242, please contact the Criminal Section of the Civil Rights Division. This article summarizes the statute to provide context for sexual misconduct prosecutions.

<sup>10</sup> § 242.

injury or included the “use, attempted use, or threatened use of a dangerous weapon, explosives, or fire,” (subject to not more than ten years in prison), or (b) that “death results from the acts . . . or if such acts include kidnapping or an attempt to kidnap, aggravated sexual abuse, or an attempt to commit aggravated sexual abuse, or an attempt to kill,” (subject to a maximum of life in prison).<sup>11</sup> The statute of limitations for a violation of Section 242 is five years unless it involves one of the latter enhancements involving death, aggravated sexual abuse, or attempts thereof, in which case there is no statute of limitations.<sup>12</sup>

## A. Color of Law and Willfulness

For the most part, law enforcement sexual misconduct investigations will focus on proving the Constitutional deprivation as well as the statutory enhancements, which is why, as discussed below, the victim interview is so essential to making the correct charging decision. Although proving color of law and willfulness can sometimes present novel issues of law and fact, it will seldom be the reason for prosecution over declination or vice versa.

With regard to the first element, acting under color of law means that the defendant was acting in his capacity as a local, state, or federal law enforcement officer, or was otherwise cloaked in the authority of the state, regardless of whether the defendant was on or off-duty.<sup>13</sup> The Criminal Section has prosecuted police officers, corrections officers, probation officers, judges, city attorneys, private prisoner transport officers, and other public officials for committing sexual misconduct under color of law.

To prove the willfulness element, the government must establish that the defendant acted with the specific intent “to deprive a person of right which has been made specific either by the express terms of the Constitution or the laws of the United States or by decision interpreting them.”<sup>14</sup> A “willful act” for purposes of Section 242 is one committed either “in open defiance or in reckless disregard of a constitutional requirement which has been made specific and definite.”<sup>15</sup> The defendant need not specifically intend the resulting constitutional deprivation, as long as the defendant intended to commit the act, the act resulted in a constitutional deprivation, and the defendant knew that what he was doing was wrong. Willfulness can also be inferred from an act that violates a clearly established constitutional right, such as sexual misconduct under color of law. That is, if the government proves that the defendant engaged in nonconsensual sexual contact with the victim, the defendant will be hard pressed to argue that he did not know that such conduct was wrong and against the law. While the defendant may argue that the conduct was consensual, as described below, that goes to whether he deprived the victim of a Constitutional right. Moreover, evidence illustrating consciousness of guilt that is often present in typical stranger or acquaintance sexual misconduct cases is also likewise often present in the law enforcement context, and serves to further bolster willfulness, e.g., threats that the victim must keep the misconduct a

---

<sup>11</sup> *Id.*

<sup>12</sup> *Id.*

<sup>13</sup> *United States v. Classic*, 313 U.S. 299, 326 (1941); *see Screws v. United States*, 325 U.S. 91, 111 (1945) (“Acts of officers who undertake to perform their official duties are included whether they hew to the line of their authority or overstep it.”); *see also Hafer v. Melo*, 502 U.S. 21, 28 (1991) (explaining color of law requirement was designed to enforce Fourteenth Amendment “against those who carry a badge of authority of a State and represent it in some capacity, whether they act in accordance with their authority or misuse it”) (citing *Scheuer v. Rhodes*, 416 U.S. 232, 243 (1974) (quoting *Monroe v. Pape*, 365 U.S. 167, 172); *West v. Atkins*, 487 U.S. 42 (U.S. 1988) (physician who was under contract with state to provide medical services to inmates at state prison hospital on part-time basis acted under color of state law and such conduct was fairly attributable to state); *Gwynn v. TransCor Am., Inc.*, 26 F. Supp. 2d 1256, 1265-66 (D. Colo. 1998) (privately-contracted transport officer acted under color of law when he sexually assaulted an inmate in his custody. But for his cloak of state authority, he would not have been able to violate her Constitutional rights.).

<sup>14</sup> *Screws*, 325 U.S. at 104.

<sup>15</sup> *Id.* at 105.

secret or face repercussions, committing the acts in secluded places or out of surveillance camera view to avoid detection, falsifying reports, and lying to local and federal authorities.

## **B. Deprivation of a Constitutional Right**

The Constitutional right at issue depends on the status of the victim at the time of the crime. As a general matter, those under arrest or those stopped by the police during an investigation are subject to the Fourth Amendment's protections against unreasonable seizure. Pretrial detainees are protected by the Due Process Clause of the Fourteenth Amendment. Convicted persons are protected by the Eighth Amendment's prohibition against cruel and unusual punishment.

### **1. Gratuitous Searches**

The right at issue does not always exactly correlate to the victim's custodial status or lack thereof. For example, the Fourth Amendment applies to pretextual or gratuitous searches of arrestees as well as inmates. Such searches are unconstitutional if done for the purpose of sexually humiliating a victim or obtaining personal sexual gratification, be it, for example, a cavity search in a locked cell of a pretrial detainee, or a search incident to arrest on the side of the road.<sup>16</sup>

### **2. Nonconsensual Sexual Contact/Sexual Assault**

Some circuits also apply the Fourth Amendment to analyze sexual assault occurring during an arrest, detention, or other "seizure."<sup>17</sup> Most circuits, however, analyze sexual assaults of non-convicted persons, regardless of whether they have been stopped by police, are under arrest, or are in custody awaiting trial, under the Due Process Clause of the Fourteenth Amendment, as a violation of fundamental bodily integrity.<sup>18</sup> To prove a violation of fundamental bodily integrity, the law enforcement officer's

---

<sup>16</sup> *Bell v. Wolfish*, 441 U.S. 520, 558 (1979) (to determine whether a search was objectively reasonable, the court balance the need for the particular search against the invasion of the personal rights that the search entailed); *Sims v. Labowitz*, No. 16-2174, 2017 WL 6031847 (4th Cir. Dec. 5, 2017) ("Sexually invasive searches require that the search bear some discernible relationship with safety concerns, suspected hidden contraband, or evidentiary need," and therefore ordering a 17-year old to masturbate in front of an officer to obtain photographs of his erect penis is objectively unreasonable). *Amaechi v. West*, 237 F.3d 356, 361 (4th Cir. 2001) (arrestee's right to be free from public, sexually intrusive search was clearly established); *Florence v. Bd. of Chosen Freeholders of Cty. of Burlington*, 566 U.S. 318 (2012) (routine strip searches of non-dangerous detainees arrested for minor offenses upheld); *Harris v. Miller*, 818 F.3d 49, 62-63 (2d Cir. 2016) ("inmates retain a limited right of bodily privacy under the Fourth Amendment. If an inmate exhibits an actual, subjective expectation of bodily privacy, and if the inmate challenges an isolated search as infringing on his or her right of bodily privacy, courts should assess the claimed violation for reasonableness under the four *Bell* factors: (1) the scope of the intrusion; (2) the manner in which it was conducted; (3) the justification for initiating it; and (4) the place in which it was conducted.").

<sup>17</sup> *See, e.g. Fontana v. Haskin*, 262 F.3d 871, 881 (9th Cir. 2001); *United States v. Langer*, 958 F.2d 522, 523-24 (2d Cir. 1992).

<sup>18</sup> *See Rogers v. City of Little Rock, Ark.*, 152 F.3d 790, 793-96 (8th Cir. 1998) (Where a woman was raped by a road patrol officer, the essence of the claim was not excessive force but a claim of "nonconsensual violation of intimate bodily integrity which is protected by substantive due process."); *Jones v. Wellham*, 104 F.3d 620, 622-23 (4th Cir. 1997) (where an officer forcibly coerced a woman into having sex in his patrol vehicle, the Fourth Amendment was inapposite because "the harm inflicted did not occur in the course of an attempted arrest or apprehension of one suspected of criminal conduct."); *see Rochin v. California*, 342 U.S. 165 (1952) (recognizing a substantive due process right to bodily integrity); *Walton v. Alexander*, 44 F.3d 1297, 1302 (5th Cir. 1995) (recognizing "[t]he right to be free of state-occasioned damage to a person's bodily integrity is protected by the Fourteenth Amendment guarantee of due process.") (Taylor Indep. Sch. Dist., 15 F.3d at 451) (en banc) (quoting *Shillingford*, 634 F.2d at 265).

conduct must be “so egregious, so outrageous, that it may fairly be said to shock the contemporary conscience.”<sup>19</sup>

Sexual assaults of convicted persons are analyzed under the Eighth Amendment as a violation of the prohibition against cruel and unusual punishment.<sup>20</sup>

### 3. Lack of Consent

Regardless of which Amendment forms the basis of the Constitutional violation, consent is a complete defense to violation of Section 242. It may seem counterintuitive that a person in custody has the ability to consent to sexual contact with the individual who has authority over her. Nonetheless, unlike some state statutes, Section 242 is not a strict liability statute. The government has to prove lack of consent, and the victim has to articulate to investigators and prosecutors that she did not consent and that the offender knew that the victim did not consent, highlighting why the victim interview is integral to developing a prosecutable case, and why the prosecutor must be well-versed in the nuances of the statute. Importantly, however, is that federal law does not require the victim to actually say the word, “no” to the perpetrator.

The key inquiry is whether the victim truly made a voluntary decision as to what she wanted to do with her body. A thorough interview will help inform as to how and why sexual contact came about. It will often be, for example, that because of the officer’s size, the remote location where the stop occurred, the fact that the officer threatened to falsely charge the victim, and a host of other factors that will only come out through a detailed interview, the victim had to submit to the officer’s advances. Submission is not consent. However, if, for example, an officer legitimately arrested the victim, the victim then chose to perform a sex act in lieu of getting arrested, and it therefore was a true quid pro quo exchange where the victim received a benefit, there is no violation of Section 242. It may otherwise be a violation of state law and, most likely, a violation of department policy, but it is not a federal civil rights crime. The same is true for an inmate who engages in sexual contact with a corrections officer in return for phone privileges, snacks from the commissary, and the like.

A significant point to keep in mind, however, is that what appears at first blush to be a quid pro quo may actually be a Section 242 violation. If the would-be victim was legitimately arrested, it is helpful to ask the victim the following during the investigative interview: What would have happened if you had told the officer, “no?” If the answer is that the officer would have legitimately arrested the victim, then the act was likely a quid pro quo, but if the answer is that the officer would have forced the victim to perform the sex act anyway, then it may very well be a federal civil rights crime. Again, a thorough interview will reveal the factors that led to the victim’s decision to perform the sex act. If the victim submitted, relented, or gave in, then the victim did not consent.<sup>21</sup> Indeed, if the victim uses the word “rape” or “sexual assault” to describe what happened, it is more likely, though not dispositive, that Section 242 is implicated.

---

<sup>19</sup> *County of Sacramento v. Lewis*, 523 U.S. 833, 846 (1998); *see also* *United States v. Guidry*, 456 F.3d 493, 498 (5th Cir. 2006) (affirming conviction of an on-duty officer who raped a woman in a secluded area); *United States v. Contreras*, 950 F.2d 232, 236 (5th Cir. 1991) (affirming conviction of an officer who sexually assaulted a woman he detained and later conspired to kill).

<sup>20</sup> *See* *Smith v. Cochran*, 339 F.3d 1205 (10th Cir. 2003) (explaining that sexual assault violates both the objective and subjective prongs of the Eighth Amendment); *Schwenk v. Hartford*, 204 F.3d 1187, 1197 (9th Cir. 2000) (“In the simplest and most absolute of terms, the Eighth Amendment right of prisoners to be free from sexual abuse was unquestionably clearly established”); *Castillo v. Day*, 790 F.3d 1013, 1018-19 (10th Cir. 2015).

<sup>21</sup> *United States v. Cobenais*, 868 F.3d 731, 739 (8th Cir. 2017) (Upholding jury instruction that states, “There is no consent if the sexual act was accomplished against the will of [the victim] by the use of force, coercion, or threats. Consent may be verbal or implied based on the facts, circumstances, and evidence presented to you.”).

Similarly, if, for example, a victim consents to a specific sexual act to get out of a legitimate arrest, but then the officer goes beyond that agreement and rapes the victim or performs an act beyond the scope of the initial consent, that subsequent act is a due process violation. Likewise, if the officer threatened to falsely charge the victim or made a false threat of a lengthy imprisonment in an effort to coerce a sex act, and the victim succumbed so that the officer would not carry out his threat, such an act violates due process.<sup>22</sup>

## C. Section 242: Felony Enhancements

The language of Section 242 provides for several enhancements that, if proven, make the constitutional deprivation a felony. The statute reads in part,

if bodily injury results or if such acts involve use, attempted use, or threatened use of a dangerous weapon, explosives, or fire . . . or if death results . . . or if such acts include kidnapping or an attempt to kidnap, aggravated sexual abuse, or an attempt to commit aggravated sexual abuse, or an attempt to kill . . .<sup>23</sup>

Acts of sexual misconduct may result in bodily injury, involve the use of dangerous weapon, or include aggravated sexual abuse and kidnapping.<sup>24</sup> As detailed throughout the section, sometimes the only way to gather evidence of these enhancements is through painstakingly thorough, detailed interviews.

### 1. Bodily Injury

To prove bodily injury, the government must establish that the victim suffered an injury to the body as a result of the defendant's actions. The defendant need not have intended to cause the injury.<sup>25</sup> The injury may be minor or temporary, including pure physical pain.<sup>26</sup>

This is significant because most sexual assaults, regardless of whether the perpetrator is in law enforcement, do not result in physical injury that can be documented. Moreover, even if vaginal injury did result, such injury tends to heal within 72 hours of the assault. It is therefore crucial that the victim immediately undergo a rape kit or similar sexual assault medical examination if the victim reports the assault within the first few days of the sexual assault. The exam could yield DNA evidence to both help identify the perpetrator and to foreclose a defense that sexual contact did not happen. As discussed below, DNA and documented injury could help prove an obstruction of justice charge where the defendant lies to state and/or federal authorities and denies sexual contact. The exam could also serve to document injuries that are consistent with the victim's account and corroborate lack of consent, while also proving the bodily injury element.

However, most reports of sexual assaults are delayed, meaning that significant physical evidence is often lost. Delayed reports occur for a variety of legitimate reasons, all of which the victim should be able to explain when asked during an investigative interview: for example, the perpetrator threatened to

---

<sup>22</sup> See *Alexander v. DeAngelo*, 329 F.3d 912, 917 (7th Cir. 2003) (holding that forcing confidential informant to have sexual contact with subject of sting operation by using false threats of lengthy imprisonment violated the confidential informant's due process rights).

<sup>23</sup> § 242.

<sup>24</sup> *Id.*

<sup>25</sup> See e.g., *United States v. Marler*, 756 F.2d 206, 216 (1st Cir. 1985) (holding that, in a Section 242 case in which death results, the government need not prove that the defendant intended the victim's death) (citing *United States v. Hayes*, 589 F.2d 811, 821 (5th Cir. 1983)).

<sup>26</sup> See *United States v. Myers*, 972 F.2d 1566, 1572-73 (11th Cir. 1992) (citing definition of "bodily injury" in statutes throughout Title 18 and finding no error in court's instruction that "bodily injury means any injury to the body, no matter how temporary," including "any burn or abrasion," bruise, or just "physical pain."). *Accord* *United States v. Gonzalez*, 436 F.3d 560, 575 (5th Cir. 2006); *United States v. Bailey*, 405 F.3d 102, 111 (1st Cir. 2005).

harm her if she reported the sexual assault; the victim did not know to whom she should report; the victim feared that she would not be believed, etc. Given the delay and the fact that most sexual assaults do not result in observable injury, it may be necessary to prove bodily injury based on “physical pain.” The victim must therefore provide specific detail of the assault because the victim is the only witness who can establish pain. Likewise, prosecutors and investigators have to ask specific, pointed questions without leading the victim. Pain can be established by asking the victim, for example, what the penetration felt like, whether the perpetrator was holding her in place and how he went about doing so, whether the victim was being restrained with handcuffs and shackles, and if the handcuffs and shackles caused pain during the assault. Previous Section 242 cases established pain in the following ways, among others: a victim’s belly chain digging into her back during the assault; the defendant tightly gripping the victim’s head as he forced her to perform a sex act; the defendant holding the victim’s arms in place such that she was left with fingerprint bruises; anal or vaginal penetration that was painful for the victim; or bleeding as a result of the assault.

## 2. Dangerous Weapon

Because law enforcement officers often carry firearms as part of their uniforms, it is not uncommon for the perpetrator to possess his gun in furtherance of the sexual assault. Establishing that the officer used his gun to further his crime will not only prove the dangerous weapon enhancement, but will also help prove that he forced the victim to submit and/or put the victim in fear of serious bodily injury, death, or kidnapping required for the Aggravated Sexual Abuse enhancement (see discussion below).<sup>27</sup> It may also give rise to a separate violation of 18 U.S.C. § 924(c).<sup>28</sup> In order to implicate Section 924(c), the underlying crime must be a crime of violence. Therefore, sexual misconduct in violation of Section 242 that only gives rise to a misdemeanor likely will not qualify. Similarly, a Section 242 violation resulting in bodily injury may also not qualify as a crime of violence. However, establishing aggravated sexual abuse—and in some circuits, the kidnapping enhancement would qualify—depends upon how each circuit defines a crime of violence and whether it is so “by its nature.”<sup>29</sup>

In some instances, perpetrators overtly use their gun during the commission of the crime by threatening to shoot the victim during or after the assault, brandishing it as a means of intimidation, or making a show of loading the bullets. However, in other instances, the perpetrators’ threats are not as overt. In *United States v. Contreras*, the Fifth Circuit Court of Appeals recognized that a law enforcement officer’s weapon can serve to both embolden the officer and coerce a victim in a sexual assault, without having to point the gun at her.<sup>30</sup> In that case, as is common in many patrol officer sexual misconduct cases, the defendant-officer drove the victim to an isolated location, stopped the car, told the victim to get out, placed his gun belt on the roof of the car, and sexually assaulted her. The court cited several factors from which the jury reasonably could have inferred that the defendant’s possession of a firearm was not “mere inadvertence,” even when there was no direct threat with the firearm: (1) the defendant was emboldened by his possession of the gun; (2) the defendant displayed the gun in order to intimidate the victim; (3) the defendant had the opportunity and ability to discharge the gun during the entire incident; and as a result (4) the victim believed the defendant would kill her if she tried to escape.<sup>31</sup> The court also

---

<sup>27</sup> 18 U.S.C. § 2241(a) (2012).

<sup>28</sup> 18 U.S.C. § 924(c) (2012) (possessing a firearm in furtherance of a crime of violence).

<sup>29</sup> See *Johnson v. United States*, 135 S. Ct. 2551 (2015); *United States v. Prickett*, 839 F.3d 697, 698 (8th Cir. 2016) (noting that “the statutory language of § 924(c)(3)(B) is distinctly narrower [than the ACCA], especially in that it deals with physical force rather than physical injury.”) (citing *United States v. Taylor*, 814 F.3d 340, 376 (6th Cir. 2016); *United States v. Moore*, 38 F.3d 977, 979 (8th Cir. 1994) (“Section 924(c)(3)(B) defines a crime as a crime of violence if ‘by its nature it involves a substantial risk that physical force against the person or property of another may be used in the course of committing the offense.’”) (citing 18 U.S.C. § 924(c)(3)(B)).

<sup>30</sup> *Contreras*, 950 F.2d at 232.

<sup>31</sup> *Id.* at 241-42.

noted that the victim “testified that she ‘had to obey him because of fear’ and that she thought he ‘would kill [her] or hit [her]’ if she attempted to run away.”<sup>32</sup>

### 3. Aggravated Sexual Abuse

In most law enforcement sexual misconduct cases, aggravated sexual abuse can be established in one of two ways as defined by 18 U.S.C. § 2241(a): “by knowingly caus[ing] another person to engage in a sexual act (1) by using force against that other person; or (2) by threatening or placing that other person in fear that any person will be subjected to death, serious bodily injury, or kidnapping; or attempting to do so . . .”<sup>33</sup>

Less commonly in the law enforcement context, aggravated sexual abuse can also be established when, as defined by 18 U.S.C. § 2241(b) the defendant:

(1) renders another person unconscious and thereby engages in a sexual act with that other person; or (2) administers to another person by force or threat of force, or without the knowledge or permission of that person, a drug, intoxicant, or other similar substance and thereby—(A) substantially impairs the ability of that other person to appraise or control conduct; and (B) engages in a sexual act with that other person; or attempts to do so . . .<sup>34</sup>

For the purposes of this enhancement and assuming the victim is at least 16-years old, a sexual act is defined under 18 U.S.C. § 2246(2) as:

(A) contact between the penis and the vulva or the penis and the anus, and for purposes of this subparagraph contact involving the penis occurs upon penetration, however slight; (B) contact between the mouth and the penis, the mouth and the vulva, or the mouth and the anus; [or] (C) the penetration, however slight, of the anal or genital opening of another by a hand or finger or by any object, with an intent to abuse, humiliate, harass, degrade, or arouse or gratify the sexual desire of any person . . .<sup>35</sup>

With regard to establishing force as set forth by Section 2241(a)(1), actual violence is not necessary.<sup>36</sup> Legislative history shows that Congress intended that “force” be defined broadly:

[t]he requirement of force may be satisfied by a showing of the use, or threatened use of a weapon [see the discussion above]; the use of such physical force as is sufficient to overcome, restrain, or injure a person; or the use of a threat of harm sufficient to coerce or compel submission by the victim.<sup>37</sup>

---

<sup>32</sup> *Id.* at 235, 241 (“Congress intended § 924(c) to apply when police officers . . . abuse the privilege of carrying a firearm by committing a crime with the weapon.”) (quoting S. Rep. No. 225, 98th Cong., 2d Sess. 315 n. 10 (1983)); Guidry, 456 F.3d at 498 (Where the defendant kept his gun belt on during the rape of a victim in a secluded area and the victim testified that she could hear the gun striking the car during the rape, but at no point did the defendant threaten her with the gun, the court commented that the gun was always within the defendant’s reach, and the court found that “[a] jury could reasonably conclude that [the defendant] was emboldened by his possession of the gun to rape [the victim], and that the gun was a threat to and intimidated [the victim].”).

<sup>33</sup> § 2241(a).

<sup>34</sup> § 2241(b).

<sup>35</sup> 18 U.S.C. § 2246(2) (2012).

<sup>36</sup> See *United States v. H.B.*, 695 F.3d 931, 936 (9th Cir. 2012); *United States v. Lauck*, 905 F.2d 15, 18 (2d Cir. 1990) (rejecting a violence requirement for § 2241).

<sup>37</sup> *Id.*

Further, “the force requirement is met when the sexual contact resulted from a restraint upon the other person that was sufficient that the other person could not escape the sexual contact.”<sup>38</sup>

Despite this broad definition of force, the mere disparity in size between the offender and the victim may not, in and of itself, be enough to prove force in the context of aggravated sexual abuse.<sup>39</sup> When interviewing the victim, it is therefore essential to determine, e.g., whether the victim felt free to resist or escape, the type of restraint, if any, the perpetrator used on the victim, whether the victim was fearful, and whether that fear was rooted in fear of death, serious bodily injury, or kidnapping, as opposed to fear of legitimately getting arrested and going to jail.

#### 4. Kidnapping

To establish the kidnapping enhancement under 18 U.S.C. § 242, the government need not prove that the defendant transported the victim across state lines. Rather, the kidnapping enhancement is analogous to false imprisonment where the victim is confined or restrained against her will.<sup>40</sup> Even if the defendant lawfully takes the victim into custody, but later keeps her confined for the purposes of sexually assaulting her, the kidnapping enhancement may be applicable.<sup>41</sup>

Considering the line of cases referenced in the previous footnote, bear in mind that the same evidence used to establish the kidnapping enhancement may also establish substantive kidnapping in violation of 18 U.S.C. § 1201.<sup>42</sup> Just like the kidnapping enhancement, there is no requirement for substantive kidnapping that the defendant transport the victim across state lines. Rather, to establish a violation of 18 U.S.C. § 1201(a), the government must prove three elements beyond a reasonable doubt: (1) the defendant knowingly and willfully seized, confined, inveigled, decoyed, kidnapped, abducted or carried away the victim; (2) the defendant held the victim for ransom, reward or some other benefit; and (3) the defendant used a means, facility or instrumentality of interstate commerce in committing the offense or in furthering its commission.<sup>43</sup>

---

<sup>38</sup> *Id.*, citing *United States v. Fulton*, 987 F.2d 631, 633 (9th Cir. 1993) (quoting *Lauck*, 905 F.2d at 18); *see also United States v. Lucas*, 157 F.3d 998, 1002 (5th Cir. 1998) (“A defendant uses force within the meaning of § 2241 when he employs restraint sufficient to prevent the victim from escaping the sexual conduct.”), *see United States v. Allery*, 139 F.3d 609, 611 (8th Cir. 1998) (holding that “force sufficient to prevent the victim from escaping the sexual contact satisfies the force element” of § 2241(a)(1)); *United States v. Webb*, 214 F.3d 962 (8th Cir. 2000) (same).

<sup>39</sup> *United States v. Bordeaux*, 997 F.2d 419, 421 (8th Cir. 1993) (Disparity in size between the defendant and the child-victim might be enough, in itself, to establish a restraint that was sufficient that the victim could not escape the sexual contact.); *United States v. Holly*, 488 F.3d 1298, 1302 (10th Cir. 2007) (“Force may be inferred by such facts as disparity in size between victim and assailant, or disparity in coercive power,” does not require “the brute force [commonly] associated with rape.”) (Internal citations omitted).

<sup>40</sup> *Guidry*, 456 F.3d 493 (Affirming the kidnapping enhancement where a police officer detained the victim, and then then drove her to a dark, wooded area and raped her, and finding that the enhancement did not require transportation across state lines, but rather is defined in a more modern, evolved form that only requires confinement.).

<sup>41</sup> *See United States v. Denny-Shaffer*, 2 F.3d 999, 1018-19 (10th Cir. 1993) (When a victim voluntarily accompanies her perpetrator but was later confined by him, the perpetrator was guilty of violating 18 U.S.C. § 1201, the federal kidnapping statute.); *United States v. Redmond*, 803 F.2d 438, 439 (9th Cir. 1986) (Merely confining a victim after she willingly began to journey with the defendant, sufficed to serve as a violation of the [kidnapping] statute even though the victim was not physically abducted or initially taken by force.); *United States v. Wesson*, 779 F.2d 1443, 1444 (9th Cir. 1986) (per curiam) (Kidnapping occurs where the victim voluntarily accompanies the defendant, but makes her desire to go home known, yet stays with defendant after he rapes her, too scared to try to escape.).

<sup>42</sup> 18 U.S.C. § 1201 (2012).

<sup>43</sup> § 1201(a).

With regard to the first element, “kidnapping” means “to unlawfully hold, keep, detain, or confine the person against that person’s will.”<sup>44</sup> “Inveigling” means to lure or lead a person astray by false representations, or by some other deceitful non-forcible means.<sup>45</sup>

With regard to proving the second element, “holds for ransom or reward or some other benefit” may be satisfied by virtually any benefit or thing that the defendant values.<sup>46</sup>

The Criminal Section has successfully charged both substantive kidnapping and the enhancement where law enforcement officers have isolated, constrained, or confined their victims in secluded locations. The kidnapping enhancement and substantive kidnapping may be particularly applicable where road patrol officers veer from their route and take victims to remote locations in deserted areas at night or out of radio range. Similarly, the enhancement may be used in prosecutions of corrections officers who lure inmates to locked closets, shower rooms, or similar areas where there are no surveillance cameras or means of being detected. Prosecutors may want to consider charging the kidnapping enhancement or substantive kidnapping where the perpetrator’s conduct does not rise to the level of aggravated sexual abuse in that the perpetrator only groped or fondled the victim. In those instances, the perpetrator’s conduct may otherwise be a misdemeanor, but for evidence that supports charging the kidnapping enhancement or substantive kidnapping, making the crime(s) a felony.

### **III. The Investigation**

#### **A. Victim Interview**

Unlike most law enforcement excessive force investigations which focus on developing law enforcement corroboration as a means to build a prosecutable case, law enforcement sexual misconduct investigations are victim-centric. Indeed, they rarely have law enforcement corroboration because sex crimes typically do not occur in front of an audience of witnesses. Therefore, the cases rise and fall with the credibility of the victim. As detailed below, in order to effectively corroborate the victim’s account, there are steps that prosecutors and investigators should take from the outset of the investigation, i.e. the very first meeting with the victim, to ensure the strength of the case.

##### **1. What to Do**

As any sex crimes prosecutor, counselor, or detective will confirm, it is not uncommon for a sexual assault victim to skip over details and minimize events during her first interview or any interview thereafter, especially if the victim is not comfortable with the prosecutor or investigator. This is especially true when investigating a potential violation of 18 U.S.C. § 242, because there is already distrust of law enforcement. These interviews take patience, time, and the ability to simultaneously be objective, fact-driven, detail-oriented, and sensitive to topics of an intimate and sometimes embarrassing nature. At the same time, it is incumbent upon the prosecutor to make the victim feel comfortable enough to disclose the entire truth, including details that both prove the elements (as set forth in the previous section), as well as “bad” facts and those facts that may be the subject of motions in limine, e.g. prior bad acts or instances

---

<sup>44</sup> See Pattern Crim. Jury Instr. 5<sup>th</sup> Cir. 2.58.

<sup>45</sup> *Id.*; See also Pattern Crim. Jury Instr. 10<sup>th</sup> Cir. 2.55 (2011); Pattern Crim. Jury. Instr. 11<sup>th</sup> Cir. 49.; See United States v. Jacques, 2011 No. 2:08-CR-117, WL 1706765, 12 (D. Vt. May 4, 2011) (noting that “a kidnapping that begins with an inveiglement and evolves into a confinement by force is one offense, not two, and begins with the inveiglement, not the confinement by force.”).

<sup>46</sup> § 1201(a); See, e.g., United States v. Williams, 998 F.2d 258 (5<sup>th</sup> Cir. 1993) (approving a charge using the term “for immoral purposes,” because “some benefit” can include sexual gratification).

of prior sexual activity.<sup>47</sup> Note that there are several exceptions under which specific instances of a victim's sexual behavior may be admissible: "(A) If the evidence is offered to prove that someone other than the defendant was the source of semen, injury, or other physical evidence; (B) If evidence of specific instances of a victim's sexual behavior is with respect to the person accused of the sexual misconduct, if offered by the defendant to prove consent or if offered by the prosecutor; and (C) If exclusion of the evidence would violate the defendant's constitutional rights."<sup>48</sup>

As prosecutors and investigators, we are trained to be skeptical, especially when the person alleging misconduct, sexual or otherwise, is in custody, is addicted to drugs, or has a lengthy criminal history, as the victims of law enforcement sexual misconduct often are and do. After all, their offenders chose them because others may question their credibility even before they begin to give their accounts. But we can maintain our objectivity and a healthy dose of skepticism without outwardly treating the victim like we do not believe her, and without placing blame, the very things the victim feared when she first decided to report the misconduct. As with any witness, we have to reconcile inconsistencies to the extent they can be reconciled, and seek answers to questions we anticipate a jury will have: for example, Why did you wait to report the misconduct?; Why did you choose to report misconduct now?; Did you try to escape, scream, fight?; Why did you not tell the state investigator all of these details when you were first interviewed?; Describe how it felt when the perpetrator penetrated you, pulled down your pants, pulled the car over; I know this is obvious, but why did you not actually say the word, "no," kick, bite, tell the first person you saw as soon as it was over?; What do you think would happen to you if you kicked, bit, or screamed for help?

For the most part, experienced prosecutors and investigators know the answers to these questions because most sex crimes committed by law enforcement follow the same pattern as sex crimes committed by teachers, bosses, babysitters, etc. But the victim needs to articulate the answers, and prosecutors and investigators need to ask the questions, not in an accusatory manner, but in an inquisitive way, designed to both put the victim at ease that she is being taken seriously and to give the case a fighting chance should there later be enough evidence to charge the offender and proceed to trial, because trial preparation begins as soon as a complaint is made. If we as prosecutors and investigators dismiss a victim's account at the outset because we deem it implausible, and then later find out that the allegation was true, we not only run the risk of losing valuable evidence because we failed to do a follow-up investigation, but we also risk irreparably destroying the victim's already-tenuous trust in the legal system.

Consider, for example, the case of a probation officer who engaged in a pattern of harassing and grooming behavior with a female probationer, culminating in groping her breasts during an office visit. The victim explained that her probation officer always kept his door open. Nonetheless, he groped her while the door was open and while there were people present in other nearby offices. Such brazen behavior on the part of the officer seemed implausible. But because prosecutors and investigators followed up on the victim's report, several other probationers came forward, the officer made recorded admissions, and he ultimately pled guilty and went to federal prison. Similarly, consider a woman who was arrested for Driving Under the Influence and was, by all accounts, intoxicated. Nevertheless, she alleged that the arresting officer pulled over on the side of the road, fondled her while she was handcuffed, put his mouth on her breast, and took pictures of her bare breasts. Investigators made it clear to the victim that they did not believe her, solidified by the subject-officer's denials that were accepted at face value by the investigators. Just prior to closing the investigation, DNA analysis revealed that the subject-officer's DNA was located inside the victim's bra cup, consistent with her account. Forensic analysis of the subject-officer's personal phone then revealed a deleted photo of the victim, bare-breasted and handcuffed in the back of the patrol vehicle. Where she was initially deemed a drunk liar, just as the

---

<sup>47</sup> See FED. R. EVID. 412, which prohibits the admissibility of prior sexual conduct for the purpose of proving that a victim engaged in other sexual behavior or to prove sexual predisposition.

<sup>48</sup> FED. R. EVID. 412(b).

subject-officer was banking on, it ultimately turned out that the victim had indeed endured an egregious assault just as she reported.

While not every allegation is true, nor will every allegation be prosecutable, investigating with objectivity will help inform which ones have merit. Doing so will further lessen the likelihood that those with merit get overlooked.

## 2. What Not to Do

The likelihood of successfully prosecuting a law enforcement sexual misconduct case is not only rooted in a solid investigation that corroborates the victim's account, but also in the consistency of the victim's account. As described above, there are many reasons why a victim may not provide all of the details during the first interview, just like there may be reasons why a victim remembers more details as time goes on, none of which bear on the truth of what happened. Experts in rape trauma and post-traumatic stress disorder can testify about traumatic memory and how traumatic events, can, for example, affect a victim's ability to recall and recount events in a chronological or linear manner.

Ideally, the victim will give one account and remain entirely consistent each time she recounts the events thereafter. Yet, even the most honest person who has not been traumatized makes inconsistent statements, even if about irrelevant details, inadvertently providing fodder for cross-examination. Where the entire case rests on the credibility of the victim, as it often does in law enforcement sexual misconduct prosecutions, there is no reason to create unnecessary inconsistencies.

Therefore, the victim should *not* testify before the federal grand jury, nor should the victim be given a polygraph examination. Neither will, by any means, strengthen the case. With regard to grand jury testimony:

- (1) No matter how consistent the victim is, she will never repeat the exact words in the same exact way at trial such that defense counsel will be unable to impeach her;
- (2) There is no reason to "lock in the victim's testimony" because unlike cooperating or reluctant witnesses, if the victim refuses to testify or if she disappears, there is no case;
- (3) Memorializing the victim's account while the victim is clear-headed or sober can be accomplished via a detailed FD-302, which the victim can use to refresh her recollection.<sup>49</sup> There is no need for a grand jury transcript. Moreover, the victim has to be clear-headed and sober to testify at trial anyway. If the victim is intoxicated at trial, there are certainly bigger issues than the victim's faulty memory;
- (4) There is no "practice" to be had by testifying before the grand jury. The grand jury is not the petit jury, and it is therefore not the proper measure of how credibly a victim will testify at trial;
- (5) Along the same lines, the purpose of the grand jury is not to test the credibility of the victim. That is the prosecutor's role;
- (6) There is no way to guarantee that grand jury testimony will be the vehicle by which to memorialize every detail of the assault in one transcript. As stated above, sometimes sexual assault victims remember details as time progresses. It is not ideal for trial, but it is the reality of handling these types of cases.

---

<sup>49</sup> FED. R. EVID. 612.

## B. Corroboration: Federal Rule of Evidence 413 and 404(b) —Similar Fact Witnesses

Federal Rule of Evidence 413 allows evidence of prior sexual assaults to be used for any matter “to which it is relevant,” including propensity, when the defendant is charged with a sexual assault.<sup>50</sup> Further, there is a presumption to allow admission of such evidence.<sup>51</sup>

Sex crimes defendants are rarely caught the first time they commit an offense. Because prior acts of sexual assault are admissible to prove propensity as well as a pattern of behavior, it is therefore advisable to focus the investigation on finding past victims in an effort to corroborate the initial victim. When offenders are probation officers or corrections officers, there is often a finite number of potential victims to whom they had access. Although time consuming, speaking with each probationer on a probation officer’s caseload or each inmate assigned to a corrections officer’s pod may mean the difference between indictment instead of declination, conviction instead of acquittal, or plea instead of trial. Similarly, for example, if the offending officer victimized a DUI arrestee or someone seeking a temporary domestic violence injunction, it may be fruitful to obtain other police reports involving DUI arrests or injunctions in an effort to identify additional victims.

Congress created Rule 413 to encourage the prosecution of sexual offenders by allowing in propensity evidence for that very reason.<sup>52</sup> As the Congressional Record set forth:

Alleged consent by the victim is rarely an issue in prosecutions for other violent crimes—the accused mugger does not claim that the victim freely handed over his wallet as a gift—the defendant in a rape case often contends that the victim engaged in consensual sex and then falsely accused him. Knowledge that the defendant has committed rapes on other occasions is frequently critical in assessing the relative plausibility of these claims and accurately deciding cases that would otherwise become unresolvable swearing matches.<sup>53</sup>

Furthermore, “since . . . rapes generally [do not] occur in the presence of credible witnesses, [FED. R. EVID. 413] permits other victims to corroborate the complainant’s account via testimony about the defendant’s prior sexually assaultive behavior . . . Corroboratory information about the defendant also limits the prejudice to the victim that often results from jurors’ tendencies to blame victims in acquaintance rape cases.”<sup>54</sup>

Nonetheless, FED R. EVID. 413 is subject to analysis pursuant to FED. R. EVID. 403 to ensure that the danger of prejudice does not substantially outweigh the probative value of uncharged conduct.<sup>55</sup> In performing the Rule 403 balancing test, courts have typically considered “the similarity of the prior acts to the acts charged . . . the closeness in time of the prior acts to the charged acts . . . the frequency of the prior acts, the presence or lack of intervening events . . . and the need for evidence beyond the testimony

---

<sup>50</sup> FED. R. EVID. 413(a).

<sup>51</sup> *United States v. Enjady*, 134 F.3d 1427, 1431 (10th Cir.1998).

<sup>52</sup> *United States v. Mound*, 149 F.3d 799, 801 (8th Cir. 1998); *United States v. Seymour*, 468 F.3d 378, 386 (6th Cir. 2006) (“Rule 413 was enacted as an exception to the default position set forth in Rule 404(b) that propensity evidence is presumptively more prejudicial than probative.”).

<sup>53</sup> *Enjady*, 134 F. 3d at 141 (citing 140 Cong. Rec. S129901–01, S12990 (R. Dole, Sept. 20, 1994)).

<sup>54</sup> FED. R. EVID. 413; *Enjady*, 134 F.3d at 1432 (citing Mark A. Sheft, *Federal Rule of Evidence 413: A Dangerous New Frontier*, 33 AM. CRIM. L. REV. 57, 69-70 (1995)); *United States v. Guardia*, 135 F.3d 1326, 1330 (10th Cir. 1998) (“[P]ropensity evidence has a unique probative value in sexual assault trials and that such trials often suffer from a lack of any relevant evidence beyond the testimony of the alleged victim and the defendant.”).

<sup>55</sup> FED. R. EVID. 413, FED. R. EVID. 403; *United States v. Strong*, 826 F.3d 1109, 1113 (8th Cir. 2016).

of the defendant and alleged victim.”<sup>56</sup> As expected, courts have frequently assigned high probative value to prior act evidence when it indicates a common pattern of behavior.<sup>57</sup>

Moreover, even when the defendant’s prior conduct does not rise to the level of sexual assault as required under Rule 413, it may still demonstrate a pattern of behavior similar to what the main victim described, and therefore be admissible under Federal Rule of Evidence 404(b) to show intent, modus operandi, common plane or scheme, or lack of mistake.<sup>58</sup> Rule 404(b) is considered “an inclusive rule, admitting all evidence of other crimes or acts except [contrary to Rule 413] that which tends to prove only criminal disposition.”<sup>59</sup> When intent is at issue, as it is to prove willfulness in Section 242 prosecutions, prior acts have been permitted to prove that element.<sup>60</sup>

It is not uncommon for sex offenders to engage in a pattern of “grooming,” in which they begin testing their victims to see how far they can push their behavior. By exploiting their victims’ weaknesses, be it substance addiction, prior victimization, or their relationship as probation officer to probationer, for example, offenders begin to push the boundaries by asking inappropriate questions or making suggestive comments, all of which may be admissible under Rule 404(b) to show his pattern and intent.

### **C. Corroboration: Outcry Witnesses**

As previously mentioned, while victims may not immediately report law enforcement sexual misconduct to the authorities, they do often disclose their assaults to friends, family members, cellmates, and the like, sometimes in person or sometimes on a recorded jail call. These disclosures are important to corroborate the victims’ tone, demeanor, and behavior after the assault. Because outcry witnesses may be nurses, counselors, or religious leaders, and do not have the same criminal history, drug addiction, etc. that afflicts the victim, their credibility is less likely to be questioned. Outcry witnesses may give details of the assault that victims were at first reluctant to disclose to investigators and prosecutors. They may have information about other victims or longtime suspicions about the offender.

Statements that victims make to outcry witnesses are also substantively admissible under Federal Rule of Evidence 801(d)(1)(B) as non-hearsay if such prior consistent statements are “offered to rebut an express or implied charge against the declarant of recent fabrication or improper influence or motive.”<sup>61</sup> More often than not, that is the very defense that the offender will put forth. In other words, it is very common for the defendant to claim that the victim is lying. In such cases, the victim’s initial disclosures to those outcry witnesses, whether they be written jail grievances or verbal statements to a pastor, are admissible for the truth of the matter asserted and go directly to proving the crime charged.

FED. R. EVID. 801(d)(1)(B) is particularly significant in the context of Rule 413 victims, where the defense may argue that the victims fabricated their accounts because they were approached by federal prosecutors and agents and wanted to be helpful in the face of their own legal problems. Jail calls, grievances, letters to family members, counseling sessions, and other disclosures to outcry witnesses are admissible to rebut such an assertion and can effectively bolster these victims’ credibility.

---

<sup>56</sup> *Guardia*, 135 F.3d at 1331 (citations omitted); *Blind-Doan v. Sanders*, 291 F.3d 1079, 1082 (9th Cir. 2002).

<sup>57</sup> *See, e.g., United States v. Benally*, 500 F.3d 1085 (10th Cir. 2007); *United States v. Crow Eagle*, 705 F.3d 325 (8th Cir. 2013).

<sup>58</sup> FED. R. EVID. 404(b).

<sup>59</sup> *United States v. Tan*, 254 F. 3d 1204, 1208 (10th Cir. 2001) (citing *United States v. Van Metre*, 150 F. 3d 339, 349 (4th Cir. 1998)).

<sup>60</sup> *Huddleston v. United States*, 485 U.S. 681 (1988); *See United States v. Mohr*, 318 F.3d 613 (4th Cir. 2003) (Similar fact evidence was properly admitted to prove that the defendant officer acted willfully when she previously used unreasonable force in a similar manner); *United States v. Dise*, 763 F.2d 586, 592 (3d Cir. 1985) (Court upheld the admissibility of a state hospital aide’s other acts of abuse because “[t]he evidence was plainly relevant on the issue of Dise’s willfulness.”).

<sup>61</sup> FED. R. EVID. 801(d)(1)(B); *Tome v. United States*, 513 U.S. 150 (1995).

## D. Subject Interview

When conducting a subject interview, there are several charging and strategic considerations to keep in mind. First, it is unlikely that a law enforcement officer will admit to engaging in sexual contact without consent. Second, unless confronted with what they perceive to be credible evidence (e.g., DNA), most law enforcement officers will deny engaging in any type of sexual contact with someone in their custody. Therefore, it is probably not strategically prudent to attempt to get the subject to admit to nonconsensual contact and then, when that fails, disclose to him that DNA was recovered. Such a disclosure will allow him to easily and falsely claim that the sex was consensual and then explain that he did not at first admit to sexual contact because he did not want to get fired.

It may be a better course of action to consider interviewing the subject early in the investigation before he learns of the state of the evidence. Despite the natural instinct to confront a subject with concrete evidence, investigators should consider not disclosing DNA evidence, but rather getting a detailed account from the subject and locking him into his story, later to be used for impeachment should he testify at trial. Investigators should focus on the specific interactions between the subject and the victim, where and why the subject took the victim to a certain location, who he saw and why he did what he is claiming to have done. By doing so, the investigative team can then work to disprove aspects of the subject's account, thereby discrediting the subject's story overall.

Importantly, even where a Section 242 violation without statutory enhancements is a misdemeanor, making material false statements to federal agents is a felony in violation of 18 U.S.C. § 1001.<sup>62</sup> Similarly, engaging in misleading conduct by lying to either state or federal investigators can be a violation of 18 U.S.C. § 1512(b)(3).<sup>63</sup> Where a subject officer falsely claims that he did not have sexual contact with anyone while on duty, in his custody, etc., it may be worth charging violations of either 18 U.S.C. § 1001 or 18 U.S.C. § 1512(b)(3) as a means of admitting uncharged conduct into evidence to prove the false statements/obstruction charge. In short, specific acts of uncharged sexual assault and misconduct would necessarily be admissible as direct evidence to prove the aforementioned false statements, obviating the need for a Rule 413 or 404(b) hearing (though filing notice of intent to admit such evidence is still good practice).

## IV. Other Statutory Violations to Consider

In addition to violations of 18 U.S.C. § 242 and its statutory enhancements, as well as other statutory violations already discussed (i.e., 18 U.S.C. §§ 924(c), 1201, 1001, 1512(b)(3)), it is worth keeping in mind other available federal statutes as investigations progress.<sup>64</sup> For example, law enforcement officers who commit sexual misconduct may falsify reports and delete messages and photographs to cover up their crimes in violation of 18 U.S.C. § 1519.<sup>65</sup>

Additionally, sexual misconduct by tribal law enforcement officers can implicate statutes for offenses committed within Indian Country pursuant to 18 U.S.C. § 1153.<sup>66</sup> Additionally, sexual assaults occurring in federal prisons implicate 18 U.S.C. §§ 2242 and 2243.<sup>67</sup> Notably unlike Section 242, Section 2243 is a strict liability crime. It is a per se violation for a corrections officers or other employees in an

---

<sup>62</sup> 18 U.S.C. § 1001 (2012).

<sup>63</sup> 18 U.S.C. § 1512(b)(3) (2012); *see* United States v. Veal, 153 F.3d 1233 (11th Cir. 1998) (finding that 18 U.S.C. § 1512(b)(3) applies to misleading conduct toward state investigators); United States v. Serrata, 425 F.3d 886, 891 (10th Cir. 2005) (applying Veal's holding to federal investigators); *see also* United States v. Anderson, 229 F. Supp. 2d 17, 22 n.3 (D. Mass. 2002).

<sup>64</sup> 18 U.S.C. §§ 242; 924(c); 1201, 1001, 1512(b)(3).

<sup>65</sup> 18 U.S.C. § 1519 (2012).

<sup>66</sup> 18 U.S.C. § 1153 (2012).

<sup>67</sup> 18 U.S.C. § 2242 (2012); 18 U.S.C. § 2243 (2012).

“institution[] or facility in which persons are held in custody by direction of or pursuant to a contract or agreement with the head of any Federal department or agency . . . [to] engage . . . in a sexual act with another person . . . in official detention; and under the custodial, supervisory, or disciplinary authority,” regardless of whether the victim consented or engaged in a quid pro quo exchange.<sup>68</sup>

Finally, when determining available statutory penalties and theories of liability, it may be prudent to coordinate with state and local law enforcement officers and prosecutors. Deferring to state prosecution or reaching a global resolution that includes both state and federal charges may best vindicate the federal interest, hold the perpetrator accountable, and be the best outcome for the victim.

## ABOUT THE AUTHOR

**Fara Gold** serves as a Special Litigation Counsel for the Criminal Section of the Civil Rights Division, where she prosecutes bias-motivated crimes and law enforcement misconduct throughout the country, with an emphasis on law enforcement sexual misconduct cases. Prior to joining the Department in 2009, Fara served as an Assistant State Attorney for nearly six years in Broward County, Florida, where she specialized in prosecuting sex crimes and child abuse cases. She is also an Assistant Adjunct Professor of Law at American University’s Washington College of Law.

---

<sup>68</sup> § 2243(b)(1)(2); *United States v. Urrabazo*, 234 F.3d 904, 907 (5th Cir. 2000) (“The term ‘detention facility’ is not limitless—it includes only those facilities designed or intended to detain prisoners. A federal courtroom does not become a federal detention facility simply because a prisoner is held in custody there during a trial or sentencing hearing. In contrast, the federal government intended the Marshals’ Service cell block to detain prisoners in the . . . federal courthouse, albeit for short periods. As a consequence, the cell block is a detention facility that qualifies as a federal prison.”).

# Can't Touch This: Payment Schedules that Prevent Obtaining Defendants' Assets for Restitution

*G. Ian Peng*  
*Attorney Advisor*  
*Asset Recovery Staff*  
*Office of Legal and Victim Programs*  
*Executive Office for United States Attorneys*

## I. Introduction

The defendant has pled guilty to mail fraud and conspiracy. As part of his judgment, and pursuant to the Mandatory Victim Restitution Act (MVRA),<sup>1</sup> the sentencing judge has ordered the defendant to pay over \$2.7 million in restitution. A year after the defendant's release from prison, he has only paid \$3,000. In an attempt to enforce and collect on the restitution obligation, the Financial Litigation Unit (FLU) of the United States Attorney's Office (USAO) discovers, and serves writs of garnishment on, two of the defendant's retirement accounts, worth roughly \$470,000 in total. However, on appeal, the circuit court points out that the sentencing judge had orally ordered the defendant to make monthly payments of only twenty-five percent of his net disposable income and did not explicitly declare the full restitution amount due and payable immediately. Indeed, the defendant has complied with the court-ordered payment schedule, however small his payments have been. As a result, the court of appeals rules that the United States cannot touch the \$470,000, despite the fact that (1) the sentencing judge apparently attempted to clarify in the written judgment that the defendant was to pay *no less than* twenty-five percent of his net *household* income; (2) 18 U.S.C. § 3613(a) states that notwithstanding any other federal law, a judgment imposing a restitution obligation may be enforced against *all* property or rights to property of the defendant; and (3) the defendant clearly had assets that could be applied towards his \$2.7 million outstanding restitution obligation. These are the facts of *United States v. Martinez*.<sup>2</sup>

In December 2015, the Tenth Circuit held in *Martinez* that the United States cannot garnish a defendant's assets beyond the amount currently due under a court-ordered payment schedule. The implications of this holding are far-reaching and can lead to the absurdity of commanding defendants to make meager payments (that potentially do not even cover interest payments on their debts) when they have additional assets that could be applied to their restitution obligations. Despite the terms set forth in a payment schedule by the sentencing court, the payment schedule amount should be considered to be a *minimum* required payment rather than the maximum that USAOs can collect at any given time. In fact, the Tenth Circuit's ruling is contrary to other circuit court decisions that have ruled on this issue—both before and since *Martinez*.

This article begins with an overview of these circuit court decisions in Part II. Next, Part III examines the Tenth Circuit's analysis and interpretation of the relevant laws in *Martinez*. Part IV considers recent district court decisions in the aftermath of *Martinez*. Lastly, Part V identifies best practices for criminal AUSAs, who are in the best position to prevent payment schedule-related problems

---

<sup>1</sup> Mandatory Victim Restitution Act, Title II of The ANTITERRORISM AND EFFECTIVE DEATH PENALTY ACT Of 1996, PL 104-132, April 24, 1996, 110 Stat 1214.

<sup>2</sup> *United States v. Martinez*, 812 F.3d 1200 (10th Cir. 2015).

from developing, as well as for FLU AUSAs, who nonetheless have tools in their enforcement arsenal to collect on defendants' restitution obligations despite payment schedules.

## II. Third, Fifth, Sixth, Seventh and Eighth Circuits: The United States May Enforce and Collect Beyond a Payment Schedule

Under the MVRA, “[a] person sentenced to pay a fine or other monetary penalty, including restitution, shall make such payment immediately, unless, in the interest of justice, the court provides for payment on a date certain or in installments.”<sup>3</sup> In *United States v. Walker*, the Second Circuit noted that “[t]he significance of . . . [a payment] schedule is diminished, however, by the fact that the victim may convert the restitution order into an abstract of judgment for the full amount of the restitution order.”<sup>4</sup> Similarly, a restitution order automatically serves as “a lien in favor of the United States on all property and rights to property” of the defendant.<sup>5</sup> Hence, victims, as well as USAOs, should be able to enforce and collect on restitution obligations beyond defendants' court-ordered payment schedules through their abstracts of judgment/liens.<sup>6</sup> The Second Circuit seemed to suggest so in *Walker* but has not directly addressed this issue.

The Seventh Circuit was the first circuit to address this issue directly. In *United States v. Fariduddin*, the defendant consented to a plea agreement that stated, “The defendant acknowledges and understands that any and all financial obligations imposed by the sentencing court are due and payable upon entry of the judgment of conviction. The defendant agrees not to request any delay or stay in payment of any and all financial obligations.”<sup>7</sup> Nevertheless, the defendant subsequently claimed that the district court entered a contradictory sentence by making restitution immediately payable in full while setting a payment schedule to begin after his release from prison.<sup>8</sup> The Seventh Circuit ruled that there was no contradiction in the defendant's sentence: the full debt was in fact immediately payable, but realizing that the defendant might not pay, the judge set a minimum installment as a condition of supervised release.<sup>9</sup> The appellate court further noted that the \$150 minimum monthly installment payments would not even cover interest payments; “\$150 per month is a floor rather than a ceiling.”<sup>10</sup>

The Seventh Circuit recently reaffirmed its holding in *Fariduddin*. In *United States v. Wykoff*, the sentencing judge specified that restitution payments were to begin immediately, and added a “special instruction”: “Any unpaid restitution balance during the term of supervision . . . shall be paid at a rate of not less than 10% of the defendant's gross monthly income.”<sup>11</sup> The defendant opposed garnishment on

---

<sup>3</sup> 18 U.S.C. § 3572(d)(1).

<sup>4</sup> *United States v. Walker*, 353 F.3d 130, 133 (2d Cir. 2003); *see also* *United States v. James*, 312 F. Supp. 2d 802, 807 (E.D. Va. 2004) (“Court-imposed payment schedules are merely one means available to enforce a restitution judgment.”); 18 U.S.C. § 3664(m)(1)(B) (“At the request of a victim named in a restitution order, the clerk of the court shall issue an abstract of judgment certifying that a judgment has been entered in favor of such victim in the amount specified in the restitution order.”).

<sup>5</sup> 18 U.S.C. § 3613(c).

<sup>6</sup> *Contra* *United States v. Villongco*, No. CR 07-9 (BAH), 2017 WL 2560905, at 4 (D.D.C. June 13, 2017) (“The government suggests that the mere existence of a lien justifies the writ of garnishment sought here, failing to acknowledge a critical difference between liens and writs of garnishment: namely, in contrast to the latter, the former merely secures debts without providing an independent means of satisfying them. Accordingly, that *all* a defendant's property may be subject to a lien does not mean that *all* a defendant's property may be garnished by the government.”).

<sup>7</sup> *United States v. Fariduddin*, 469 F.3d 1111, 1112 (7th Cir. 2006).

<sup>8</sup> *Id.* at 1113.

<sup>9</sup> *Id.*

<sup>10</sup> *Id.*

<sup>11</sup> *United States v. Wykoff*, 839 F.3d 581, 582 (7th Cir. 2016).

the basis that he had already forfeited two of his homes and the USAO had seized money from his prison account.<sup>12</sup> Despite these assets being insufficient to pay his restitution obligation in full, he argued that collection of the balance should be postponed to his release on account of the judge’s “special instruction,” which he alleged limited his restitution payments to ten percent of his monthly income.<sup>13</sup> The Seventh Circuit, however, recognized that “the instruction doesn’t say that; it says that ten percent is the *minimum* amount he must pay to complete restitution.”<sup>14</sup> The Seventh Circuit further reasoned:

The federal criminal code *requires* that restitution be paid immediately unless the district court provides otherwise, 18 U.S.C. § 3572(d)(1), which it did not. In *United States v. Sawyer*, 521 F.3d 792, 795 (7th Cir. 2008), we pointed out that at the start of incarceration “any existing assets should be seized promptly. If the restitution debt exceeds a felon’s wealth, then the Mandatory Victim Restitution Act of 1996, 18 U.S.C. §§ 3663A, 3664, demands that this wealth be handed over immediately.”<sup>15</sup>

The Fifth Circuit reached a similar conclusion in *United States v. Ekong*.<sup>16</sup> Upon the USAO’s application, the district court had issued a writ of garnishment upon the defendant’s interest in pension benefits.<sup>17</sup> On appeal, the defendant argued that immediate payment was not required since the judgment provided for restitution payments in installments.<sup>18</sup> The Fifth Circuit disagreed:

This argument is without merit. “The [Mandatory Victim Restitution Act (MVRA)] provides the Government authority to enforce victim restitution orders in the same manner that it recovers fines and by all other available means” and, under 18 U.S.C. § 3613(a), it may collect “restitution ‘in accordance with the practices and procedures for the enforcement of a civil judgment under Federal law or State law,’” including the Federal Debt Collection Procedures Act of 1990.<sup>19</sup>

Thus, the Fifth Circuit has also recognized that a sentencing court’s imposition of a payment schedule does not prevent the United States from pursuing the defendant’s assets. After all, the MVRA requires the Attorney General to enforce restitution orders “aggressively.”<sup>20</sup>

The Third Circuit followed suit in an unpublished opinion, *United States v. Shusterman*.<sup>21</sup> Again, the defendant argued that the district court erred in ordering garnishment, given that it had already set a payment schedule at sentencing.<sup>22</sup> Like in *Ekong*, the Third Circuit cited 18 U.S.C. § 3613(a) as support for allowing the United States to enforce a restitution order via garnishment.<sup>23</sup> The Third Circuit then pointed out that the judgment made restitution *due immediately*, but in the event that restitution had not been paid in full before the commencement of the defendant’s term of supervised release, the judgment directed the defendant to start making monthly installment payments.<sup>24</sup> Hence, “[t]he District Court did not err in allowing garnishment as an additional means to collect the restitution judgment.”<sup>25</sup> However,

---

<sup>12</sup> *Id.*

<sup>13</sup> *Id.*

<sup>14</sup> *Id.* (citing Fariduddin, 469 F.3d at 1113).

<sup>15</sup> *Id.*

<sup>16</sup> *United States v. Ekong*, 518 F.3d 285 (5th Cir. 2007).

<sup>17</sup> *Id.* at 286.

<sup>18</sup> *Id.*

<sup>19</sup> *Id.* (quoting *United States v. Phillips*, 303 F.3d 548, 550-51 (5th Cir. 2002)).

<sup>20</sup> *Id.* (quoting *Phillips*, 303 F.3d at 551).

<sup>21</sup> *United States v. Shusterman*, 331 F. App’x 994 (3d Cir. 2009).

<sup>22</sup> *Id.* at 996.

<sup>23</sup> *Id.*

<sup>24</sup> *Id.* at 996-97.

<sup>25</sup> *Id.* at 997.

the Third Circuit also implied that garnishment may not have been appropriate if the judgment had not provided that restitution was due immediately.<sup>26</sup>

Similarly, the Sixth Circuit ruled in *United States v. Schwartz* that a payment schedule did not change the fact that restitution was due immediately upon entry of judgment.<sup>27</sup> In this case, the district court made the defendant's restitution obligation to a victim hospital due immediately whereas restitution to the Internal Revenue Service was due upon his release to supervision.<sup>28</sup> The district court also ordered the defendant to make periodic payments if he held a job while incarcerated.<sup>29</sup> The Sixth Circuit affirmed the district court's order enforcing a writ of garnishment, reasoning that "[b]ecause Schwartz did not pay that portion of the restitution due to [the victim hospital] at the time the judgment was imposed, that amount became an unpaid debt that the government could seek to collect immediately by all available and reasonable means."<sup>30</sup>

In yet another unpublished opinion, *United States v. Behrens*, the Eighth Circuit also held that a payment schedule did not preclude garnishment because the judgment specified that restitution was due in full immediately.<sup>31</sup> The Eighth Circuit further noted that "the judgment imposed the obligation to make installment payments without limiting the government's ability to institute civil collections proceedings."<sup>32</sup> Unfortunately, the court did not expound upon its reasoning in reaching this conclusion.

### III. Tenth Circuit: The United States Cannot Enforce and Collect Beyond a Payment Schedule

In contrast, the Tenth Circuit ruled in *United States v. Martinez* that the United States cannot garnish a defendant's assets when he is in compliance with his payment schedule.<sup>33</sup> While the defendant was paying the court-ordered monthly installments, the USAO served writs of garnishment for two of the defendant's retirement accounts.<sup>34</sup> The USAO argued that it could garnish the retirement accounts to satisfy the entire restitution judgment.<sup>35</sup> In concluding that the defendant had no obligation to pay the full amount immediately, provided that he complied with the payment schedule, the Tenth Circuit pointed to the fact that the installment schedule only called for monthly payments and the district court did not order immediate payment in full.<sup>36</sup>

Specifically, the district court had *orally* ordered the defendant to make monthly payments of twenty-five percent of his net disposable income.<sup>37</sup> However, in its *written* judgment, the district court

---

<sup>26</sup> *Id.* at 997 n.2 ("United States v. Roush, 452 F. Supp. 2d 676 (N.D. Tex. 2006), relied upon by Shusterman, is distinguishable. The court granted a motion to quash garnishment where the judgment provided that restitution would be paid pursuant to the payment schedule but did not provide that restitution was due immediately."). *But cf.* United States v. Rostan, 565 F. App'x 798, 801 (11th Cir. 2014) ("The default payment schedule for all orders of restitution requires a defendant to make immediate payment. 18 U.S.C. § 3572(d)(1) . . . The restitution order is only required to include a payment schedule 'if other than immediate payment is permitted under section 3572(d).' *Id.* § 3612(b)(1)(D)").

<sup>27</sup> United States v. Schwartz, 503 F. App'x 443, 446 (6th Cir. 2012).

<sup>28</sup> *Id.* at 445.

<sup>29</sup> *Id.*

<sup>30</sup> *Id.* at 446.

<sup>31</sup> United States v. Behrens, 656 F. App'x 789, 790 (8th Cir. 2016).

<sup>32</sup> *Id.*

<sup>33</sup> Martinez, 812 F.3d at 1202.

<sup>34</sup> *Id.* at 1201.

<sup>35</sup> *Id.* at 1202.

<sup>36</sup> *Id.* at 1203-04.

<sup>37</sup> *Id.* at 1203.

ordered the defendant to pay “no less than 25% of the net household income.”<sup>38</sup> Noting that the oral pronouncement controls in situations where the oral and written orders conflict, the Tenth Circuit found that “[n]othing in the oral pronouncement suggests that the district court intended to make the full restitution amount due immediately.”<sup>39</sup> Furthermore, the Tenth Circuit pointed out that in its written judgment, the district court did not check the box in a section of the judgment form entitled “Schedule of Payments” to indicate that the restitution award was due “[i]n full immediately.”<sup>40</sup>

The Tenth Circuit also analyzed the statutory provisions governing restitution orders and, likewise, concluded that an installment-based restitution order does not create an immediately enforceable debt for the entire amount.<sup>41</sup> The appellate court first considered 18 U.S.C. § 3572(d)(1), which provides that “[a] person sentenced to pay . . . restitution . . . shall make such payment immediately, *unless*, in the interest of justice, the court provides for payment . . . in installments.”<sup>42</sup> The Tenth Circuit interpreted § 3572(d)(1) as imposing a dichotomy: *either* immediate payment in full *or* installment payments.<sup>43</sup> “This subsection implies that full payment is due immediately *only if* the district court does not provide for installment payments.”<sup>44</sup> The Tenth Circuit further justified its interpretation by citing 18 U.S.C. § 3572(i):

Subsection (i) of § 3572 explains what happens when a defendant defaults on a restitution order. Under § 3572(i), a defendant who defaults on a payment schedule must pay the full restitution award within 30 days, “notwithstanding any installment schedule.” *Id.* § 3572(i). This provision would be unnecessary, even meaningless, if the total restitution amount were already owed in full under an installment-based restitution order.<sup>45</sup>

In addition, the Tenth Circuit cited 18 U.S.C. § 3664(f)(2),<sup>46</sup> which requires a sentencing court to consider the defendant’s financial condition in setting a payment schedule.<sup>47</sup> “In requiring the court to consider the defendant’s financial condition, the statute directs the court (not the government) to determine how and when the defendant should pay the restitution amount . . . [The government’s contrary] interpretation would allow the government to usurp the district court’s role.”<sup>48</sup>

The Tenth Circuit distinguished the Fifth Circuit’s decision in *United States v. Ekong*<sup>49</sup> by highlighting that Ekong would trigger the payment schedule only if she had not paid restitution in full by the time she began supervised release.<sup>50</sup> Moreover, the Tenth Circuit opined:

It is impossible to tell from the *Ekong* opinion whether the Fifth Circuit reached this conclusion because it (1) agreed with the government that the judgment required immediate payment of the full restitution amount, requiring installments only if the defendant failed to pay the full amount by the time she began supervised release or (2) concluded that the

---

<sup>38</sup> *Id.*

<sup>39</sup> *Id.*

<sup>40</sup> *Id.* at 1204.

<sup>41</sup> *Id.* at 1204-05.

<sup>42</sup> *Id.* at 1205 (quoting 18 U.S.C. § 3572(d)(1)).

<sup>43</sup> *Id.*

<sup>44</sup> *Id.*

<sup>45</sup> *Id.*

<sup>46</sup> 18 U.S.C. § 3664(f)(2) directs the court to consider “(A) the financial resources and other assets of the defendant, including whether any of these assets are jointly controlled; (B) projected earnings and other income of the defendant; and (C) any financial obligations of the defendant; including obligations to dependents” in setting a payment schedule.

<sup>47</sup> Martinez, 812 F.3d at 1206.

<sup>48</sup> *Id.*

<sup>49</sup> Ekong, 518 F.3d 285.

<sup>50</sup> Martinez, 812 F.3d at 1207.

government could garnish the full restitution amount in all cases, regardless of the language in the restitution order.

If the Fifth Circuit was relying on the government's argument that the installment schedule was conditional, the argument would not apply to the oral pronouncement of Mr. Martinez's restitution order. And if the Fifth Circuit was relying on the statutory scheme, the court failed to explain how that scheme would permit garnishment of payments not yet due. Thus, we do not believe *Ekong* helps us decide whether the government was entitled to garnish Mr. Martinez's retirement accounts in the absence of a default on his payment schedule.<sup>51</sup>

The Eighth Circuit, in turn, distinguished *Martinez* from its decision in *United States v. Behrens* by pointing out that the restitution order in *Martinez* did not create an immediately enforceable debt for the full restitution amount.<sup>52</sup>

#### IV. Post-*Martinez*

Most district court opinions that have considered *Martinez* in deciding the United States' ability to enforce and collect beyond a payment schedule appear to turn on whether or not the judgment at hand specifies that restitution is due in full immediately. For example, in *United States v. Kay*,<sup>53</sup> the United States District Court for the District of Minnesota—which is in the Eighth Circuit—followed the Tenth Circuit's *Martinez* decision rather than the Eighth Circuit's (unpublished) *Behrens* decision due to its factual similarity to the *Martinez* case. As in *Martinez*, the sentencing court had ordered that restitution be paid according to the payment schedule set forth in the judgment, which was silent as to when the full amount was due.<sup>54</sup> The court declared that “[s]ince the judgment in this case specified that [the defendant’s] repayment was due only in installments, the full restitution amount was not due immediately.”<sup>55</sup> The court further found “[t]he Government’s reliance upon the laconic reasoning of *Ekong* . . . [to be] unpersuasive in light of other authority reasoning why ‘due immediately’ language in the judgment is critical.”<sup>56</sup>

Comparably, the United States District Court for the Northern District of Oklahoma—which is in the Tenth Circuit—found *Martinez* to be inapposite in *United States v. Daniels*, a case in which the judgment indicated a payment schedule but also made the entire restitution amount due in full immediately.<sup>57</sup> Here, the court explicitly stated that “[n]otwithstanding establishment of a payment schedule, nothing shall prohibit the United States from executing or levying upon property of the defendant discovered before or after the date of this Judgment.”<sup>58</sup> Consequently, the court denied the defendant's motion to prohibit the United States from taking her tax refund.<sup>59</sup>

---

<sup>51</sup> *Id.* at 1208. Although the Fifth Circuit admittedly provides a sparse analysis in *Ekong*, it did observe that the United States may collect “restitution ‘in accordance with the practices and procedures for the enforcement of a civil judgment under Federal law or State law’”—including the Federal Debt Collection Procedures Act of 1990 (FDCPA)—pursuant to 18 U.S.C. § 3613(a). *Ekong*, 518 F.3d at 286. A writ of garnishment is one of the FDCPA post-judgment remedies available to the United States. *See* 28 U.S.C. § 3205.

<sup>52</sup> *Behrens*, 656 F. App'x at 790.

<sup>53</sup> *United States v. Kay*, No. CR 11-218(1) ADM/TNL, 2017 WL 875784 (D. Minn. Mar. 3, 2017).

<sup>54</sup> *Id.* at 3.

<sup>55</sup> *Id.* at 4.

<sup>56</sup> *Id.* at 3.

<sup>57</sup> *United States v. Daniels*, No. 15CR0096001CVETLW, 2017 WL 1538457, at 3 (N.D. Okla. Apr. 28, 2017).

<sup>58</sup> *Id.* at 1.

<sup>59</sup> *Id.* at 4.

Likewise, in *United States v. Barber*, the United States District Court for the Northern District of Illinois distinguished its case from *Martinez* by emphasizing that both its oral pronouncements at sentencing as well as its written judgment made clear that the defendant was ordered to pay restitution in full immediately; the defendant was to pay monthly installments of at least ten percent of her net monthly income only if any amount remained unpaid at the commencement of her supervised release.<sup>60</sup> “The monthly installment is a floor, not a ceiling, and nothing in the Court’s order prevents the government from attempting to collect the amount due by means other than and in addition to the installment payments.”<sup>61</sup>

In a similar vein, the criminal judgment in *United States v. Rush* called for installment payments during the defendant’s term of incarceration, but also provided that the “total criminal monetary penalties are due immediately” and that “[a]ny installment schedule shall not preclude enforcement of the restitution or fine order by the United States under 18 U.S.C. §§ 3613 and 3664(m).”<sup>62</sup> The United States District Court for the Western District of Virginia reasoned that both the text of the judgment as well as 18 U.S.C. § 3613 supported the government’s execution of its lien on the defendant’s inmate trust account:

[T]he point of the payment schedule was to allow [the defendant] access to a small amount of funds for commissary items while he is incarcerated . . . It was never the intention of the court, in setting up the payment schedule, to give Rush’s then-unliquidated boat asset a free pass from being subject to execution by the government.<sup>63</sup>

Alternatively, the court found that the sale of the defendant’s boat and the resultant deposit of \$15,571.28 into his inmate trust account constituted a material change in economic circumstances affecting his ability to pay.<sup>64</sup>

Conversely, the United States District Court for the District of Columbia has found that “immediately payable” does not supplant the payment schedule and is merely boilerplate language.<sup>65</sup> In *United States v. Villongco*, the USAO sought to garnish the defendant’s retirement and brokerage accounts, which the Pre-Sentence Investigation Report had previously disclosed.<sup>66</sup> At the defendant’s sentencing hearing, the judge ordered that “[t]he special assessment and restitution are immediately payable to the clerk of this court,” while also specifying that the defendant “must pay the balance of any restitution owed at a rate of no less than \$500 each month” as a special condition of supervised release.<sup>67</sup> When the defense counsel sought clarification as to when payments would begin, the sentencing judge stated, in relevant part, “the payments for the restitution as well as the special assessments are due and payable immediately,” but “[t]he fact is that, you know, payment schedules end up getting worked out when people don’t have the full amount of all that’s due and payable immediately.”<sup>68</sup>

---

<sup>60</sup> *United States v. Barber*, No. 14 CR 601-2, 2016 WL 4377136, at 1 (N.D. Ill. Aug. 17, 2016).

<sup>61</sup> *Id.* (citing *Fariduddin*, 469 F.3d at 1113). However, the court declined to address whether the United States could immediately enforce and collect the entire restitution amount in all cases, regardless of the language at sentencing and in the written judgment. *Id.* at 2 (“The Court need not wade into the parties’ arguments about the breadth of the Government’s power to collect criminal judgments and whether *Martinez* was wrongly decided with respect to that power because this Court concludes that, in this particular case, the Government’s attempts to execute the judgment against the funds in the IRAs and the life insurance policies are consistent with the terms of the sentence imposed by this Court and the plea agreement defendant entered into.”).

<sup>62</sup> *United States v. Rush*, No. 5:14CR00023, 2016 WL 3951224, at 1 (W.D. Va. July 20, 2016).

<sup>63</sup> *Id.* at 3.

<sup>64</sup> *Id.*

<sup>65</sup> *United States v. Villongco*, No. CR 07-009 (BAH), 2016 WL 3747508, at 9 (D.D.C. July 11, 2016).

<sup>66</sup> *Id.* at 1.

<sup>67</sup> *Id.* at 2.

<sup>68</sup> *Id.*

The USAO argued that the payment schedule merely established *minimum* monthly payments and does not obviate the defendant’s liability for payment of restitution in full, in accordance with the MVRA as well as the oral pronouncement at sentencing.<sup>69</sup> The court rejected that “any provision or purpose of the MVRA permits the government to ignore the specific terms of the restitution order, including, in particular, a payment schedule imposed after consideration of the requisite statutory factors concerning the economic circumstances of the defendant.”<sup>70</sup> Most critically, the district court found that the payment schedule language required the defendant to pay restitution “at a rate of no less *or more* than \$500.00 each month,” pursuant to binding precedent from the D.C. Circuit.<sup>71</sup> Furthermore, the time had passed for the USAO to seek garnishment of these investment accounts: “If the government wanted to recover the defendant’s assets held by Fidelity Investments, ‘it was incumbent on the government to speak up at . . . [sentencing], rather than accepting the Court’s ruling without objection and then attempting to circumvent it by garnishment.’”<sup>72</sup> Ultimately, the court found that the “immediately payable” language did not supersede the monthly payment schedule.<sup>73</sup> Upon the United States’ motion for reconsideration, the court further opined that “[i]n light of [the] constitutional concern [regarding ordering defendants to pay amounts of money they simply do not have], the MVRA’s requirement that full restitution be ordered is, by necessity, aspirational in nature.”<sup>74</sup>

## V. Combatting *Martinez* and Its Progeny

As the preceding case law demonstrates, criminal AUSAs’ actions in drafting plea agreements and during sentencing are critical to the FLUs’ success (or failure) in enforcing and collecting on restitution obligations beyond court-ordered payment schedules. So as to avoid problems associated with payment schedules, the preferred method of payment is clearly an immediate lump sum payment of the restitution judgment and, for any remaining balance due, the general imposition of restitution, with payment due and to begin immediately. To that end, AUSAs should inform courts of all known assets belonging to defendants at the time of sentencing and advocate for immediate lump sum payments via these assets.

In cases for which courts set payment schedules, such payment schedules should be considered to be a “floor”—not a “ceiling”—for our collection efforts. USAOs should continue to enforce restitution orders, even when defendants are current on their payment schedules. However, the *Martinez* decision illustrates the importance of ensuring that oral judicial pronouncements clearly state the terms of defendants’ restitution payments, especially with regards to restitution being due in full immediately.<sup>75</sup>

---

<sup>69</sup> *Id.* at 7.

<sup>70</sup> *Id.*

<sup>71</sup> *Id.* at 8 (where a restitution order states that “‘the balance of any restitution [is] owed at a rate of not less than \$50 each month,’ . . . [t]hat statement, however, must mean that a rate of not less *or more* than \$50 each month was required.”) (quoting *United States v. Hughes*, 813 F.3d 1007, 1009 (D.C. Cir. 2016)).

<sup>72</sup> *Id.* (quoting *Roush*, 452 F. Supp. 2d at 682).

<sup>73</sup> *Id.* at 9.

<sup>74</sup> *Villongco*, 2017 WL 2560905, at 8.

<sup>75</sup> *See Martinez*, 812 F.3d at 1203-04. Nevertheless, Tenth Circuit precedent also dictates that courts cannot order that restitution be “due in full immediately” unless the defendant actually has the ability to pay in full immediately. *See, e.g., United States v. Ahidley*, 486 F.3d 1184, 1191 (10th Cir. 2007) (vacating a restitution payment schedule, which stated that restitution was due immediately, since “[n]othing in the record . . . indicates that the district court engaged in the requisite consideration of . . . Mr. Ahidley’s financial resources.”); *United States v. Zunie*, 444 F.3d 1230, 1238 (10th Cir. 2006) (finding that the district court erred in ordering the full amount of restitution due immediately without regard to the defendant’s indigence); *United States v. Garcia-Castillo*, 127 F. App’x 385, 393 (10th Cir. 2005) (“The presentence report noted that Garcia-Castillo had no income or assets and only a grade-school education. As conceded by government counsel at oral argument, the district court violated [18 U.S.C. § 3664(f)(1)–(3)] by ordering the full amount of restitution due immediately without contemplating the defendant’s

Hence, at the outset, it is crucial for AUSAs to include express terms in plea agreements that any payment schedule imposed is merely a minimum (thereby thwarting potential objections to garnishments and other enforcement activities), and to affirmatively advocate for the appropriate payment schedule language at sentencing. AUSAs should ensure that defendants are advised at sentencing that (1) any schedule is a minimum expectation (i.e., all criminal monetary penalties are due immediately), (2) the defendant is expected to pay whatever is possible at all times, and (3) the government’s collection is not limited to the payment schedule (e.g., “[Any] payment schedule shall not preclude enforcement of the restitution or fine order by the United States under 18 U.S.C. §§ 3613 and 3664(m)”<sup>76</sup>).

Nonetheless, even if both the plea agreement and the oral pronouncement at sentencing clearly state that restitution is “due and payable immediately,” this still may not overcome some courts’ interpretation of this language as “boilerplate,” as in *Villongco*.<sup>77</sup> The case of *United States v. Grigsby*<sup>78</sup> illustrates a work-around to both the failure of a judgment to provide explicitly for immediate payment in full as well as courts’ potential interpretation of “due and payable immediately” language as being boilerplate. As in *Martinez*, the district court in *Grigsby* concluded that the judgment authorized only monthly payments, given that the judgment addressed installment payments but failed to provide for immediate payment.<sup>79</sup> However, the USAO also argued that garnishment was warranted because the defendant failed to mention his union pension plan—the asset that it sought to garnish—in the financial statement that he submitted to the probation office.<sup>80</sup> The court agreed that the defendant failed to comply with 18 U.S.C. § 3664(d)(3), which requires that defendants owing restitution provide a full accounting of their finances.<sup>81</sup> That is to say, the defendant had misled the court at the time of sentencing:

But for Grigsby’s unjustified and illegal concealment of the pension plan, the court would have issued an immediate order of full restitution at the time of sentencing . . . “Discovery of previously unknown or hidden assets [may] constitute a change in the defendant’s economic circumstances that could justify modification under section 3664(k), as it would be a change in the economic circumstances presented to the court at sentencing.”<sup>82</sup>

---

ability to pay, a payment schedule, or nominal payments.”). Thus, at least in the Tenth Circuit, “due immediately” is only available if the record establishes the defendant’s ability to pay immediately.

<sup>76</sup> See Rush, 2016 WL 3951224, at 1.

<sup>77</sup> Villongco, 2016 WL 3747508, at 9.

<sup>78</sup> *United States v. Grigsby*, No. 12-10174-JTM, 2016 WL 1056560 (D. Kan. Mar. 16, 2016), *aff’d*, *United States v. Grigsby*, 665 F. App’x 701 (10th Cir. 2016).

<sup>79</sup> *Id.* at 2.

<sup>80</sup> *Id.* at 3.

<sup>81</sup> *Id.*

<sup>82</sup> *Id.* at 3-4 (quoting Roush, 452 F. Supp. 2d at 681 n.6).

Consequently, the court ruled that the defendant's economic circumstances had changed pursuant to 18 U.S.C. § 3664(k),<sup>83</sup> and the United States was entitled to an order for immediate payment in full, in the interests of justice.<sup>84</sup>

Alternatively, the district court also found that 18 U.S.C. § 3664(n)<sup>85</sup> authorized immediate payment in full.<sup>86</sup> The court asserted that “[w]hile the statute generally is designed to reach any ‘windfall’ received by a person under a restitution requirement [while incarcerated], the language of the statute is broad, and applies where a defendant obtains ‘substantial resources’ after the initial order of restitution ‘from any source.’”<sup>87</sup> Here, the defendant gained access to substantial resources that were not previously available to him and concealed from the court.<sup>88</sup>

As *Grigsby* demonstrates, if the court deems a payment schedule to be appropriate and assets of the defendant are subsequently discovered, the USAO should strongly consider filing a motion requesting that the court order an immediate lump sum payment or at least raise the payment plan pursuant to 18 U.S.C. §§ 3664(k) and/or 3664(n). Such § 3664(k) and § 3664(n) motions should effectively acquire defendants’ newly discovered assets, regardless of whether or not the sentencing court had designated a payment schedule or declared that restitution is due and payable immediately.

---

<sup>83</sup> 18 U.S.C. § 3664(k) states:

A restitution order shall provide that the defendant shall notify the court and the Attorney General of any material change in the defendant's economic circumstances that might affect the defendant's ability to pay restitution. The court may also accept notification of a material change in the defendant's economic circumstances from the United States or from the victim. The Attorney General shall certify to the court that the victim or victims owed restitution by the defendant have been notified of the change in circumstances. Upon receipt of the notification, the court may, on its own motion, or the motion of any party, including the victim, adjust the payment schedule, or require immediate payment in full, as the interests of justice require.

*See also* 18 U.S.C. § 3572(d)(3):

A judgment for a fine which permits payments in installments shall include a requirement that the defendant will notify the court of any material change in the defendant's economic circumstances that might affect the defendant's ability to pay the fine. Upon receipt of such notice the court may, on its own motion or the motion of any party, adjust the payment schedule, or require immediate payment in full, as the interests of justice require.

<sup>84</sup> *Grigsby*, 2016 WL 1056560 at 5, *aff'd*, *Grigsby*, 665 F. App'x at 708 (“where, as here, the court finds that a defendant failed to disclose (or knowingly concealed) assets at sentencing that would affect his ability to pay restitution, on later discovery of those assets, the court may modify its order of restitution as the interests of justice require pursuant to 18 U.S.C. § 3664(k).”).

<sup>85</sup> 18 U.S.C. § 3664(n) states: “If a person obligated to provide restitution, or pay a fine, receives substantial resources from any source, including inheritance, settlement, or other judgment, during a period of incarceration, such person shall be required to apply the value of such resources to any restitution or fine still owed.”

<sup>86</sup> *Grigsby*, 2016 WL 1056560 at 5. On appeal, the Tenth Circuit affirmed the district court's order on the basis that the district court had correctly held that the discovery of the concealed retirement account qualified as a change in economic circumstances under 18 U.S.C. § 3664(k) and did not reach the alternative argument regarding 18 U.S.C. § 3664(n). *Grigsby*, 665 F. App'x at 706.

<sup>87</sup> *Grigsby*, 2016 WL 1056560 at 5 (citation omitted).

<sup>88</sup> *Id.*

Finally, 18 U.S.C. § 3572(i) provides, in relevant part, that “[n]otwithstanding any installment schedule, when a fine or payment of restitution is in default, the entire amount of the fine or restitution is due within 30 days after notification of the default.” Thus, any payment schedule is extinguished in the event the defendant defaults, and the USAO can accordingly enforce upon the entire restitution amount.

#### **ABOUT THE AUTHOR**

□ **G. Ian Peng** is an Attorney Advisor on the Office of Legal and Victim Programs’ Asset Recovery Staff at the Executive Office for United States Attorneys (EOUSA). He serves as an EOUSA point-of-contact for the Financial Litigation Units of the United States Attorneys’ Offices on issues pertaining to financial litigation, criminal restitution, and civil collections. Prior to joining EOUSA, Mr. Peng served as an Assistant District Attorney in the Office of the District Attorney, Bronx County, New York.

Page Intentionally Left Blank

# Marital Privilege in Domestic Violence and Child Abuse Cases in Federal Courts: Exceptions to the Privilege and Compelling Testimony

*Sasha N. Rutizer*

*Trial Attorney*

*Human Rights and Special Prosecutions*

*United States Department of Justice*

*Ex turpi causa non oritur actio*

Latin- “from a dishonorable cause an action does not arise.”

## I. Introduction

Domestic violence and child abuse often occur inside the home, outside the presence of others, and depend on secrecy, shame, and fear. These reasons and untold others frequently keep victims from reporting their abuse. When victims do come forward, they are often faced with internal and external pressure not to testify against their abuser. What happens when the best evidence or the only evidence of a crime comes from the victim? In cases of domestic violence and child abuse, this is all too often true. In these cases, defendants may seek to prevent the introduction of the most damaging evidence against them by asserting that anything their victim-spouse would testify about is privileged. As well, the victim-spouse may even claim marital privilege and refuse to cooperate or testify.

As an initial matter, it is important to recognize that the term marital privilege actually encompasses two distinct privileges—adverse testimony and marital communications.<sup>1</sup> The adverse testimony privilege allows a spouse to refuse to testify against the defendant-spouse. However, the privilege only exists during the lifetime of the marriage; thus, divorce and often separation will negate it.<sup>2</sup> The breadth of the privilege includes statements made prior to or during the marriage. The marital communications privilege “bars testimony concerning statements privately communicated between spouses.”<sup>3</sup> Either spouse may assert the marital communications privilege, and it survives termination of the marriage.

Prosecutors faced with cases involving an assertion of marital privilege by either spouse would benefit from understanding the development of the marital privilege in common law, the breadth and limitations of the marital privilege as they exist today, and how courts have handled the issue of whether a

---

<sup>1</sup> The adverse testimony privilege has also been referred to as the anti-marital facts privilege. Likewise, the marital communications privilege has also been referred to as the confidential communications privilege. For simplicity this article solely uses adverse testimony and marital communications.

<sup>2</sup> There are a number of other instances in which the privilege does not apply, though they are beyond the scope of this article.

<sup>3</sup> *United States v. Marashi*, 913 F.2d 724, 729 (9th Cir. 1990).

victim-spouse can be compelled to testify.<sup>4</sup> As a general matter, prosecutors will find that courts do not recognize the marital privilege in domestic violence and most child abuse cases, whether it is invoked by defendants or their spouses. Thus, in many instances, a witness spouse can, in fact, be compelled to testify like any other witness.

But because marital privilege and its exceptions have developed through common law, courts have not been consistent in the application and underlying analyses on which the privilege has been recognized or rejected. Considerable clarity and uniformity in application could be achieved by codifying the marital privilege, perhaps by modeling it after the “husband-wife” privilege found in Military Rule of Evidence 504.

## II. Recognition in Common Law of the Marital Privilege and Its Exceptions in Spouse-as-Victim Cases

Unlike most states and even the military, the marital privilege is not specifically enumerated in the Federal Rules of Evidence.<sup>5</sup> Most privileges recognized by federal courts<sup>6</sup> come from the language contained in Rule 501 that “[t]he common law—as interpreted by United States courts in the light of reason and experience—governs a claim of privilege unless [the U.S. Constitution, federal statute, or rules prescribed by the Supreme Court] provides otherwise.”<sup>7</sup> To that end, understanding the origin of the marital privilege and its ensuing treatment sheds light on contemporary holdings that no privilege exists in domestic violence and most child abuse cases.

Common law prescribed that a man could not testify on his own behalf, given his obvious self-interest. Moreover, archaic rationale dating back to the 1600s dictated that a woman had no distinct legal existence apart from her husband.<sup>8</sup> It followed, therefore, that a wife was similarly disqualified from testifying on behalf of, or against, her husband. Until at least 1933, this rationale served as the basis for the rule that one spouse was incompetent to testify in the other’s criminal trial. In 1933, the Supreme Court abrogated part of the rule and recognized that a spouse could testify on behalf of the other spouse in federal court.<sup>9</sup> The Court reasoned that whatever public policy justified the rule in the first place was no longer applicable, and “[t]he public policy of one generation may not, under changed conditions, be the

---

<sup>4</sup> See generally *United States v. Byrd*, 750 F.2d 585 (7th Cir. 1984). A decision to compel a victim of abuse to testify should balance the potential impact on an individual victim with the prosecutor’s obligation to represent the interests of the community as a whole. For a more detailed treatment of this issue visit [http://www.aequitasresource.org/Issue\\_9\\_Walking\\_A\\_Tightrope\\_Balancing\\_Victim\\_Privacy\\_and\\_Offender\\_Accountability\\_in\\_Domestic\\_Violence\\_and\\_Sexual\\_Assault\\_Prosecutions\\_Part\\_I\\_May\\_2013.pdf](http://www.aequitasresource.org/Issue_9_Walking_A_Tightrope_Balancing_Victim_Privacy_and_Offender_Accountability_in_Domestic_Violence_and_Sexual_Assault_Prosecutions_Part_I_May_2013.pdf) as well as [http://www.aequitasresource.org/Issue\\_10\\_Walking\\_A\\_Tightrope\\_Balancing\\_Victim\\_Privacy\\_and\\_Offender\\_Accountability\\_in\\_Domestic\\_Violence\\_and\\_Sexual\\_Assault\\_Prosecutions\\_Part\\_II\\_May\\_2013.pdf](http://www.aequitasresource.org/Issue_10_Walking_A_Tightrope_Balancing_Victim_Privacy_and_Offender_Accountability_in_Domestic_Violence_and_Sexual_Assault_Prosecutions_Part_II_May_2013.pdf) (last visited November 17, 2017).

<sup>5</sup> For a compilation on state treatment of this issue visit <http://www.aequitasresource.org/> (last visited December 11, 2017).

<sup>6</sup> The only privilege specifically enumerated in the Federal Rules of Evidence is the attorney-client privilege. FED. R. EVID. 502.

<sup>7</sup> Conversely, Mil. R. Evid. 504, specifically lays out the husband-wife privilege and its exceptions.

<sup>8</sup> *Trammel v. United States*, 445 U.S. 40, 44 (1980) (citing 8 J. Wigmore, *Evidence* § 2227 (McNaughton rev. 1961)).

<sup>9</sup> *Funk v. United States*, 290 U.S. 371, 378-79 (U.S. 1933). Over time, legal scholars argued that this broad marital privilege should be narrowed to only confidential marital communications, rather than an outright ability to foreclose testimony. After all, “[c]ertain exemptions from . . . giving testimony are recognized by all courts. But every such exemption is grounded in a substantial individual interest which has been found, through centuries of experience, to outweigh the public interest in the search for truth.” *United States v. Bryan*, 339 U.S. 323, 331 (1950).

public policy of another.”<sup>10</sup> It followed, then, that one spouse was permitted to testify on behalf of the other. However, the Court in *Funk* did nothing to vitiate the adverse testimony part of the rule, and continued to recognize the general principle that one spouse could prevent the other from testifying against him. Accordingly, what was once an absolute bar of incompetency became more of a privilege a spouse could choose to invoke when it benefited them.<sup>11</sup> That is to say, when a wife’s testimony could help her defendant-husband, she could be permitted to testify. However, public policy still supported precluding her adverse testimony if it could harm her husband.

Notwithstanding the general rule that a wife could not adversely testify against her husband, courts, including the Supreme Court, recognized an exception in cases where the husband committed an offense against the wife.<sup>12</sup> Thus, even the earliest affirmation of a marital privilege that prevented one’s spouse from testifying adversely against the other always recognized an exception in cases where one spouse was a victim of the other.

### III. Distinguishing Between a Witness-Spouse and Victim-Spouse is Essential to Understanding the Application of Marital Privilege

The distinction between victim and witness can sometimes be murky, but the distinction is critical in the application of the marital privilege. As an illustration, consider *United States v. Hawkins*, a 1958 Mann Act prosecution under 18 U.S.C. § 2421 that alleged the transportation of a girl from Arkansas to Oklahoma for immoral purposes.<sup>13</sup> There, the trial court allowed the government to use Hawkins’ wife as an adverse witness against him.<sup>14</sup> The Supreme Court reversed the conviction, stating that “[w]hile the rule forbidding testimony of one spouse *for* the other was supported by reasons which time and changing legal practices had undermined, we are not prepared to say the same about the rule barring testimony of one spouse *against* the other.”<sup>15</sup> The *Hawkins* Court also noted that the adverse testimony privilege belonged to both spouses, and that either could assert the privilege.<sup>16</sup> To be clear, the wife in *Hawkins* was not the victim; rather, she possessed certain incriminatory information regarding Hawkins’s actions. To be sure, the Court in *Hawkins* was fully aware of the ‘crime against the spouse’ exception dating back to *Stein*.<sup>17</sup> In this instance, the Court did not consider the charged offense to be a crime against the spouse, and therefore the general rule forbidding one spouse from testifying against the other (absent the consent of both parties) controlled.

Conversely, consider *Wyatt v. United States*. In *Wyatt*, unlike in *Hawkins*, the husband was prosecuted for a violation of the Mann Act when he brought his wife over state lines for purposes of prostituting her. Wyatt’s wife was compelled to testify, over her objection, and Wyatt was thereafter

---

<sup>10</sup> *Id.* at 381, quoting *Patton v. United States*, 281 U.S. 276, 306 (1930).

<sup>11</sup> Departing from the notion that a wife had no independent status, the rationale behind what came to be known as the marital privilege was the paternalistic view that the sanctity of a marriage should be protected, even if that came at the expense of getting to the truth.

<sup>12</sup> See *Stein v. Bowman*, 38 U.S. 209, 217 (1839) (noting that “neither husband nor wife can be a witness for or against each other. [But] this rule is subject to some exceptions, as when the husband commits an offence against the person of his wife.”). See also *State v. Smith*, 9 Ohio Dec. 749, 749-50 (1898) (“At common law, the rule was that husband and wife were not competent witnesses for or against each other . . . there was one exception, and that was in a case where the husband was charged with committing a crime against the person of his wife.”).

<sup>13</sup> *Hawkins v. United States*, 358 U.S. 74, 74 (1958).

<sup>14</sup> The Court did not address the issue of compelling the wife, because she did not object to testifying at trial.

<sup>15</sup> *Hawkins*, 358 U.S. at 77 (emphasis added).

<sup>16</sup> *Id.* at 78.

<sup>17</sup> The *Hawkins* Court commented that “the rule yielded to exceptions in certain type of cases . . . [as in] ‘where the husband commits an offence against the person of his wife.’” *Hawkins*, 358 U.S. at 75, quoting *Stein*, 38 U.S. at 221.

convicted.<sup>18</sup> The Supreme Court granted certiorari to further consider its analysis in *Hawkins*. First, the Court addressed the defendant's objection to his wife's testimony, holding that "it cannot be seriously argued that one who has committed this 'shameless offense against wifeness,' should be permitted to prevent his wife from testifying to the crime by invoking an interest founded on the marital relation or the desire of the law to protect it."<sup>19</sup> Effectively, the Court dismissed the defendant's attempt to invoke the adverse testimony privilege. The Court then turned to the issue of compelling the wife to testify against her will, stating:

[n]either can we hold that, whenever the privilege is unavailable to the party, it is ipso facto lost to the witness as well. It is a question in each case, or in each category of cases, whether, in light of the reason which has led to a refusal to recognize the party's privilege, the witness should be held compellable. Certainly, we would not be justified in laying down a general rule that both privileges stand or fall together.<sup>20</sup>

So, the Court reasoned, just because the defendant's claim to the privilege had been defeated, it did not follow that the wife's marital privilege (to refuse to testify) was also extinguished. Upon further examination, the Court considered the argument that "where the wife has chosen not to 'become the instrument' of her husband's downfall, it is her own privilege which is in question, and the reasons for according it to her in the first place are fully applicable."<sup>21</sup> However, in affirming that the victim-spouse did not have a privilege in this instance, the Court ultimately reasoned that the policy behind the Mann Act was controlling. "A primary purpose of the Mann Act was to protect women who were weak from men who were bad."<sup>22</sup> In applying that rationale, the Court held "it not an allowable choice for a prostituted witness-wife 'voluntarily' to decide to protect her husband by declining to testify against him."<sup>23</sup> Thus, where the spouse is a victim, not only can she choose to testify against her defendant-spouse, she may also be compelled to do so.<sup>24</sup>

Accordingly, these two Supreme Court cases illustrate that in criminal cases, an abusive/criminal spouse cannot benefit from his own bad conduct by invoking the marital privilege against adverse testimony and thereby silence his victim-spouse. Moreover, even if the victim-spouse does not wish to testify against her abuser-spouse, she may be compelled to do so.

---

<sup>18</sup> *Wyatt v. United States*, 362 U.S. 525, 526 (1960).

<sup>19</sup> *Id.* at 527.

<sup>20</sup> *Id.* at 529.

<sup>21</sup> *Id.* at 529-30.

<sup>22</sup> *Id.* at 530, quoting *Denning v. United States*, 247 F. 463, 465 (5th Cir. 1918).

<sup>23</sup> *Id.*

<sup>24</sup> In an earlier case consistent with the Supreme Court's ruling in *Wyatt*, the Eighth Circuit permitted a wife to testify against her husband in a case in which she was transported by him for purposes of prostitution. *Shores v. United States*, 174 F.2d 838 (8th Cir. 1949). Interestingly, though not surprisingly, on cross examination the wife stated that her husband did not coerce her into prostitution, that she did not want him prosecuted, and that she did not want to testify against him. On appeal, the court handled this by noting:

[n]or does the fact that appellant's wife stated on the stand that she did not wish to testify against her husband in any way affect the situation. As a matter of fact, she did not refuse to testify, so as to require the court to compel her to do so, but, even if she had, this would have made no difference. So far as appellant's rights were concerned, the wife's testimony, as we have indicated, was competent evidence against him, and no legal ground was available to him for objection to it. And the wife herself, like any other witness, was without privilege in the situation to say whether she did or did not wish to testify.

*Id.* at 841.

## IV. Marital-Privilege in Child Abuse Cases

By extension, courts have broadened their analysis to hold that no marital privilege exists in child abuse cases. Just as public policy demands that a defendant-spouse not benefit from his own misconduct by silencing the victim-spouse when he injures her, neither can he benefit by silencing his spouse when he injures a child. For example, in 1975, the United States Court of Appeals for the Eighth Circuit upheld a trial court’s decision to permit the testimony of the defendant’s wife in his trial for rape of their twelve-year-old daughter, over his objection.<sup>25</sup> At the outset, the court reasoned that it (and all federal courts) “has the right and the responsibility to examine the policies behind the federal common law privileges and to alter or amend them when ‘reason and experience’ so demand.”<sup>26</sup> In affirming the conviction, the court listed five reasons why “the exception to the [adverse testimony] privilege for offenses committed against a spouse should be expanded to include crimes done to a child of either spouse.”<sup>27</sup> The five reasons the court gave were: 1) serious crimes against a child are an offense against the family and thus inimical to fostering family peace; 2) parental testimony in child abuse cases is necessary given the statistical likelihood that the abuse took place in the home; 3) “any rule that impedes the discovery of truth in a court of law impedes as well the doing of justice;” 4) strong state court authority supports the premise that a crime against a child is also a crime against the spouse; and 5) the development of a sea change in state law “rendering the marital privilege unapplicable [sic] in cases of charged child abuse and neglect.”<sup>28</sup>

Simply, in cases where family members are abused at the hands of a defendant-spouse, he cannot then seek to shield his criminal conduct by cloaking himself with the marital privilege (designed to promote family harmony) by preventing his wife’s testimony.<sup>29</sup>

Table 1- Pre 1980	Adverse Testimony	Marital Communications
Which Party Can Invoke	Either	Either
Exception in Domestic Violence Cases	Yes	Yes
Exception in Child Abuse Cases	Yes	Probably
Government Can Compel Adverse Spousal Testimony in Domestic Violence Cases	Yes	Yes
Government Can Compel Adverse Spousal Testimony in Child Abuse Cases	Unknown	Unknown

Table 1 illustrates the state of the law at the time of the *Allery* decision.

## V. *Trammel* and Its Subsequent Interpretation of Marital Privilege

While the law seemed settled with respect to application of the marital privilege in spousal and child abuse cases, in 1980 the Supreme Court decided *Trammel v. United States*, which has since thrown

<sup>25</sup> *United States v. Allery*, 526 F.2d 1362 (8th Cir. 1975).

<sup>26</sup> *Id.* at 1366.

<sup>27</sup> The facts of *Allery* only contemplated adverse testimony, and thus the court did not address marital communications. *Id.* at 1362.

<sup>28</sup> *Id.* at 1366-67.

<sup>29</sup> Examination of available case law prior to 1980 does not shed much light on how courts delineated between adverse testimony and marital communications in child abuse prosecutions.

application of the privilege into confusion.<sup>30</sup> Trammel was prosecuted by the government for narcotics trafficking, and during the course of his trial, he attempted to assert marital privilege in order to prevent his wife (an unindicted, immunized co-conspirator) from testifying adversely against him. Trammel's wife was deeply involved in the criminal enterprise, but after a routine customs search revealed four ounces of heroin on her person, she agreed to cooperate with the government. The District Court ruled that Trammel's wife could testify on behalf of the government but not with respect to any marital communications.<sup>31</sup> On direct appeal, Trammel argued that allowing his wife to testify over his objection constituted reversible error in light of the holding in *Hawkins*. Stated differently, Trammel argued that *Hawkins* stood for the proposition that *both* spouses must consent to the presentation of adverse testimony, and since he objected to his wife's adverse testimony, she should have been barred from providing it. After losing on direct appeal, Trammel persisted in this argument to the Supreme Court.

Ultimately, the Supreme Court modified the old rule requiring both spouses to consent to waiver of the adverse spousal testimony privilege and now vested the privilege in only the witness-spouse.<sup>32</sup> In rejecting Trammel's claim, the Court found that the "ancient foundations" for the privilege (a wife had no separate existence apart from her husband) had disappeared, and the "contemporary justification" (promotion of family harmony) which vested the privilege in both spouses, likewise, was absent when one spouse was *willing* to testify against the other.<sup>33</sup> It followed that allowing the defendant-spouse to assert the privilege "seems far more likely to frustrate justice than to foster family peace."<sup>34</sup>

Arguably, the holding in *Trammel* was the natural next-step in the evolution of marital privilege cases because of the developing recognition that a wife was independent of her husband and that a defendant-spouse may not benefit from his own misconduct. However, in reaching its holding that the privilege should rest solely with the witness-spouse, the Court also stated "the witness may be neither compelled to testify nor foreclosed from testifying."<sup>35</sup> Thus, despite the fact that the *Trammel* Court was singularly addressing its holding in *Hawkins* (a witness-spouse case), some have seized on this language to argue that it altered the landscape in marital-privilege cases by holding that regardless of whether a spouse is a witness to, or a victim of, her spouse's crimes, she cannot be compelled to testify if she declines to cooperate or participate.<sup>36</sup>

---

<sup>30</sup> Trammel, 445 U.S. 40.

<sup>31</sup> *Id.* at 43.

<sup>32</sup> In so doing, the Court acknowledged that recognition of privileges has an adverse effect on obtaining the truth, and the rationale for allowing such a discordant impact requires "a public good transcending the normally predominant principle of utilizing all rational means for ascertaining truth." *Id.* at 50, quoting *Elkins v. United States*, 364 U.S. 206, 234 (1960).

<sup>33</sup> *Id.* at 52. ("When one spouse is willing to testify against the other in a criminal proceeding . . . there is probably little in the way of marital harmony for the privilege to preserve.")

<sup>34</sup> *Id.* at 52-53. The Court noted the government could be dissuaded from offering such leniency if the defendant-spouse could control his wife's testimony, thus "the privilege can have the untoward effect of permitting one spouse to escape justice at the expense of the other."

<sup>35</sup> *Id.* at 53.

<sup>36</sup> To be clear, the *Trammel* Court distinguished the adverse spousal testimony privilege from the marital communications privilege. "It is essential to remember that the *Hawkins* privilege is not needed to protect information privately disclosed between husband and wife in the confidence of the marital relationship . . . [t]hose confidences are privileged under the independent rule protecting confidential marital communications. *Id.* at 51, citing *Blau v. United States*, 340 U.S. 332 (1951). Notwithstanding this observation, the Court did hint that an exception might also apply to marital communications. Trammel, 445 U.S. at 46 n.7.

## VI. Lack of Clarity After *Trammel* Results in Disparate Holdings in Domestic Violence and Child Abuse Cases

The fallout from differing interpretations of *Trammel* has provided fertile ground for defendants to once again argue for the application of marital privilege in domestic violence and child abuse cases. For instance, in 2011, Tavares Chandler sought to exclude oral and written statements his wife made at his trial for being a felon-in-possession of a handgun. Chandler was arrested on this charge because his wife called the police to report that he had beaten her and her daughter in the three days prior to the call, and that he had pulled a gun on her. Chandler moved the court to exclude her statements because he *anticipated* his wife would invoke her privilege not to testify against him. In support of his motion, Chandler argued that the holding in *Trammel* “was designed to afford a witness-spouse the *opportunity* to testify in circumstances in which he or she was victimized, not to give the Government the ability to compel the witness-spouse’s testimony.”<sup>37</sup> In denying the motion, the district court held “[a]s the Supreme Court has noted, instances of domestic violence are ‘notoriously susceptible to intimidation or coercion of the victim to ensure that she does not testify at trial.’”<sup>38</sup> The court found that it could not say in this instance, whether Chandler’s wife’s refusal to testify was “voluntary.”<sup>39</sup> However, in examining the impact of the *Trammel* language (“may be neither compelled to testify nor foreclosed from testifying”), the court understood it to be narrowly tailored, and “merely . . . nonbinding dicta” and proclaimed that “this Court would still be bound by *Wyatt*,” which was directly on point.<sup>40</sup>

Turning to another recent example in a domestic violence setting, in 2017 the United States Court of Appeals for the Ninth Circuit decided *United States v. Seminole*, where the defendant asserted, in light of *Trammel*, that his wife could not be compelled to testify in his trial for strangling and assaulting her.<sup>41</sup> At trial, the victim-spouse “made clear in a variety of ways that she wanted no part of this prosecution.”<sup>42</sup> The government called her anyway, and she asserted the adverse spousal privilege. Citing the longstanding exception to the privilege, the district court compelled her testimony. While testifying, she provided a markedly different account than what she told law enforcement. Thereafter, the government impeached her with prior inconsistent statements and obtained a conviction. On appeal, Seminole claimed the district court erred in compelling his wife’s testimony, arguing that the Supreme Court’s language in *Trammel*—that the witness spouse “may be neither compelled to testify nor foreclosed from testifying”—controlled. The court addressed the longstanding history of the “spouse as victim” exception and noted that “[h]undreds of years of adverse and ironclad precedent normally end a case. But Seminole argues that the Supreme Court in *Trammel*, dramatically altered the spousal privilege landscape.”<sup>43</sup> In dispensing with his argument, the court stated that:

Seminole reads too much into this language. If a court says that hearsay is inadmissible without noting its countless exceptions, this does not reflect an intent to eliminate the exceptions. Similarly, it is clear from the context of *Trammel* that the Court was not overruling *Wyatt* with these 12 words. Rather, it was simply stating the general principle that, absent an exception, a witness cannot be compelled to testify against her spouse.<sup>44</sup>

---

<sup>37</sup> *United States v. Chandler*, 2011 WL 1871223, at 3 (D. Nev. May 16, 2011) (emphasis added).

<sup>38</sup> *Id.* at 4, quoting *Davis v. Washington*, 547 U.S. 813, 833 (2006).

<sup>39</sup> *Id.*

<sup>40</sup> *Id.* at 5 (holding an unwilling victim-spouse can be compelled to testify).

<sup>41</sup> *United States v. Seminole*, 865 F.3d 1150 (9th Cir. 2017).

<sup>42</sup> *Id.* at 1151.

<sup>43</sup> *Id.* at 1153.

<sup>44</sup> *Id.* at 1153-54.

In affirming the district court’s ruling, the *Seminole* court concluded that domestic violence “is a crime that is ‘notoriously susceptible to intimidation or coercion of the victim to ensure that she does not testify at trial.’”<sup>45</sup>

Since *Allery* and *Trammel*,<sup>46</sup> a number of other circuits have similarly found that no privilege exists (either marital communications or adverse testimony) in cases of child abuse where a child of either spouse, and in some instances, any child, was the victim. For example, in 1997, the United States Court of Appeals for the Tenth Circuit recognized “an exception to the [marital communications] privilege for crimes committed against a minor relative in the defendant’s household.”<sup>47</sup> The *Bahe* court reasoned that there was no difference, from a policy perspective, between crimes committed against children of the married couple, a step-child, or a relative visiting the home. Indeed, child abuse “generally occurs in the home . . . and is often covered up by the innocence of small children and by threats against disclosure.”<sup>48</sup> The court concluded “it would be unconscionable to permit a privilege grounded on promoting communications of trust and love between marriage partners to prevent a properly outraged spouse with knowledge from testifying against the perpetrator.”<sup>49</sup> Likewise, the United States Court of Appeals for the First Circuit has held that “the ‘offense against spouse’ exception to the marital communications privilege must be read to cover an offense against a child of either spouse in order to further the privilege’s underlying goals of promoting marital and family harmony.”<sup>50</sup> Shortly thereafter, the United States Court of Appeals for the Sixth Circuit adopted the reasoning articulated in both *Breton* and *Bahe* and found no marital communications privilege exists in cases of child abuse (even when the victim was the defendant’s step-granddaughter).<sup>51</sup> The United States Courts of Appeal for the Fifth and Ninth Circuit have reached a similar result.<sup>52</sup>

On the other hand, notwithstanding its decision in *Bahe*, the Tenth Circuit also decided *United States v. Jarvison*, where it declined to “create an exception to the spousal testimonial privilege in cases of child abuse . . . [or] to create an exception—not currently recognized by any federal court—allowing a court to compel adverse spousal testimony.”<sup>53</sup> Arguably, the court erred in its statement that no other federal court had theretofore allowed a court to compel adverse spousal testimony.<sup>54</sup> Furthermore, it seems incongruous that the same court would find an exception to the marital communications privilege (arguably the most sacred of the privileges) but not also find an exception to the adverse spousal testimony privilege, which allows for testimony about actions and statements not made within the confines of the marital partnership.<sup>55</sup>

---

<sup>45</sup> *Id.* at 1154, quoting Davis, 547 U.S. at 832–33.

<sup>46</sup> Importantly, contained within *Trammel* is a nod to the *Allery* holding, recognizing the expansion of the exception in cases of crimes against children. *Trammel*, 445 U.S. at 46 n.7.

<sup>47</sup> *United States v. Bahe*, 128 F.3d 1440, 1441 (10th Cir. 1997).

<sup>48</sup> *Id.* at 1446.

<sup>49</sup> *Id.*

<sup>50</sup> *United States v. Breton*, 740 F.3d 1, 12 (1st Cir. 2014).

<sup>51</sup> *United States v. Underwood*, 859 F.3d 386, 392 (6th Cir. 2017).

<sup>52</sup> See *United States v. Cameron*, 556 F.2d 752, 755-56 (5th Cir. 1977) (recognizing the long understood exception to marital privilege in prosecutions for crimes committed by one spouse against the other or against the children of either); *United States v. White*, 974 F.2d 1135, 1138 (9th Cir. 1992) (using the same rationale in *Allery* regarding adverse testimony, and holding “[s]imilarly, the marital communications privilege should not apply to statements relating to a crime where a spouse or a spouse’s children are the victims.”).

<sup>53</sup> *United States v. Jarvison*, 409 F.3d 1221, 1231 (10th Cir. 2005).

<sup>54</sup> *Accord*, Wyatt, 362 U.S. 525; Shores, 174 F.2d 838.

<sup>55</sup> Adding to the confusion of the *Jarvison* opinion, the Tenth Circuit, a full seven years earlier, held:

[i]t is unnecessary for us to consider Mr. Castillo’s argument [that the court violated his privilege to be free from the *adverse testimony* of his spouse, because] . . . during the pendency of his appeal, this court decided *Bahe*, in which ‘we recognized an exception to the *marital communications*

Similarly, consider the Ninth Circuit’s decision in *United States v. Banks*, that a grandchild was not the functional equivalent of a child of either spouse, and thus, finding that the marital communications privilege applied to prevent the witness spouse from testifying.<sup>56</sup> Here, the defendant was convicted of possession, production, transportation, and receipt of child pornography wherein one video included Banks and his two-year-old grandson. Despite recognizing the validity of *Allery* and *White*, the *Banks* court found that “although these facts demonstrate a strong bond between the victim and his grandparents, they do not show the type of relationship that would be considered the functional equivalent of a birth or step-child’s relationship with his parents.”<sup>57</sup>

Accordingly, the landscape of the exception to marital privilege in cases of child abuse post-*Trammel* is nebulous, and the facts surrounding the relationship to the child have proven paramount.

Table 2- Post <i>Trammel</i>	Adverse Testimony	Marital Communications
Which Party Can Invoke	<i>Only Witness-Spouse</i>	Either
Exception in Domestic Violence Cases	Yes	Yes
Exception in Child Abuse Cases	Yes*	Yes*
Government Can Compel in Domestic Violence Cases	<i>Probably</i>	<i>Probably</i>
Government Can Compel in Child Abuse Cases	<i>Circuit Split</i>	<i>Circuit Split</i>

\* Depends on the Circuit and facts surrounding the relationship with the child.

Table 2 illustrates the fallout and confusion post-*Trammel*.

While domestic violence cases may have reached an equilibrium in the consistency of judicial application in the marital privilege and its exceptions, child abuse cases clearly have not. The inconsistent and piecemeal rationale set forth in the foregoing decisions for when an exception to the marital privilege should be recognized in child abuse cases is a compelling argument for a more coherent and consistent approach.

## VII. Recommendation for a Codified Federal Rule of Evidence on Marital Privilege

In light of the foregoing, an enumerated privilege, such as that found in Military Rule of Evidence 504, would certainly offer more clarity and consistency in application of the marital privilege and its exceptions in federal courts. Military Rules of Evidence, unlike the Federal Rules, are prescribed by the President of the United States, and therefore, interpretations based on common law are inapplicable in

---

privilege for spousal testimony relating to the abuse of a minor child within the household.’ Because Mr. Castillo’s case falls within the exception outlined by *Bahe*, Mrs. Castillo’s testimony did not violate the privilege.

*United States v. Castillo*, 140 F.3d 874, 884-85 (10th Cir. 1998) (emphasis added). What is unusual about the *Castillo* opinion, and by extension *Jarvison*, is that Mr. Castillo was arguing adverse spousal testimony privilege, *Bahe* dealt with marital communications, but the court appears to be saying an exception exists in either instance when it comes to spousal testimony relating to abuse of a minor child within the home.

<sup>56</sup> *United States v. Banks*, 556 F.3d 967 (9th Cir. 2009).

<sup>57</sup> *Id.* at 976.

military courtrooms.<sup>58</sup> Rather, military courts look to a specifically enumerated privilege, its exceptions, and definitions when ruling on its applicability. To that end, the husband-wife privilege enshrined in Military Rule of Evidence 504 recognizes two distinct privileges—spousal incapacity (adverse testimony) and confidential communications (marital communications). Similar to federal jurisprudence, the witness-spouse alone has the privilege to refuse to testify adversely against his or her spouse, and the privilege does not survive termination of the marriage.<sup>59</sup> Likewise, the marital communications privilege can be claimed by either spouse, and it survives the marriage.<sup>60</sup>

Dissimilar from federal jurisprudence, specific language exists in the military rule regarding the exception in domestic violence and child abuse cases:

There is no privilege . . . [i]n proceedings in which one spouse is charged with a crime against the person or property of the other spouse or a child of either, or with a crime against the person or property of a third person committed in the course of committing a crime against the other spouse.<sup>61</sup>

Helpfully, the rule also includes a definition of “child of either:”

‘A child of either’ means a biological child, adopted child, or ward of one of the spouse and includes a child who is under the permanent or temporary physical custody of one of the spouse, regardless of the existence of a legal parent-child relationship.<sup>62</sup>

‘Temporary physical custody’ means a parent has entrusted his or her child with another. There is no minimum amount of time necessary to establish temporary physical custody, nor is a written agreement required. Rather, the focus is on the parent’s agreement with another for assuming parental responsibility for the child. For example, temporary physical custody may include instances where a parent entrusts another with the care of their child for recurring care or during absences due to temporary duty or deployments.

An enumerated privilege that includes specific exceptions and definitions would prove exceedingly helpful to both practitioners and courts alike. While there is still room for debate regarding individual factual scenarios in “temporary physical custody” situations, federal jurisprudence would be better served by adopting such language.

## VIII. Conclusion

As the foregoing illustrates, fertile ground still exists for defense counsel to argue for the application of marital privilege in both domestic violence and child abuse cases. A prepared prosecutor has both case law and policy arguments on her side when advocating that no privilege exists, and should be ready to address the history and trend of this ever-narrowing privilege in these types of cases. As an illustration, if presented with a defense argument that while some federal circuits have carved out exceptions for marital communications, few have specifically addressed adverse spousal testimony

---

<sup>58</sup> *United States v. Custis*, 65 M.J. 366, 368-69 (C.A.A.F. 2007).

<sup>59</sup> MIL. RULE EVID. 504(a).

<sup>60</sup> MIL. RULE EVID. 504(B).

<sup>61</sup> MIL. RULE EVID. 504(c)(2)(A).

<sup>62</sup> Military Rule of Evidence 504 was amended in 2007 “to more broadly define a ‘child of either.’” *United States v. Slape*, 76 M.J. 501, 505 (A.F. Ct. Crim. App. 2016). Prior to 2007, the rule did not encompass a “de facto child exception.” *Id.*, quoting *United States v. McCollum*, 58 M.J. 323, 340 (C.A.A.F. 2003). The *McCollum* court therefore found appellant’s admission to his wife that he raped her fourteen-year-old sister to be privileged. *McCollum*, 58 M.J. at 338.

exceptions in child abuse cases, a strong counter argument may include:

- the affirmative case law on the topic;
- the longstanding exception in cases of spousal abuse;
- the public policy behind the privilege—including why defendant’s actions extinguish his ability to be protected by the privilege—and state court treatment;<sup>63</sup> and
- facts specific enough to illustrate that the child at issue is the type of child contemplated by the public policy.

However, the ideal outcome given the inconsistency in application, would be for the Supreme Court to revisit the issue of marital privilege or for the privilege to be codified in the federal rules by adopting the language of Military Rule of Evidence 504, which cogently addresses the privilege and exceptions. Ultimately, a uniform understanding and application of the marital privilege and its exceptions will affirm the societal recognition of promoting family harmony without allowing this noble goal to be exploited by those defendants whose criminal conduct has already seriously undermined the harmony of the family by victimizing their spouse, children, or others in the family unit.

#### **ABOUT THE AUTHOR**

□ **Sasha N. Rutizer** is a Trial Attorney in the Human Rights and Special Prosecutions Section of the Criminal Division, where she prosecutes international violent crime, transnational alien smuggling, and human rights abuses. Prior to joining DOJ, Sasha taught best-practices in child abuse prosecution at the National District Attorneys Association. Before that she served in the Army Judge Advocate General’s Corps as a special victim prosecutor, government appellate attorney, and defense attorney. Presently, as a reservist in the JAG Corps, Sasha serves as the senior law clerk for the nine-judge Army Court of Criminal Appeals, located at Ft. Belvoir, Virginia.

*The author wishes to thank Marissa Brodney, a 3L at Harvard Law School who contributed to the research for this article while serving as a summer law intern at HRSP.*

---

<sup>63</sup> In appropriate circumstances, we may also argue “privileges created by state courts and applicable state statutes.” Allery, 526 F.2d at 1365.

Page Intentionally Left Blank

# Coming Soon to a Theater Near You—Motions to Prevent the Cross Examination of Defense Experts

*James D. Peterson*  
*Trial Attorney*  
*Capital Case Section*

“Even if one does not completely agree with Wigmore’s assertion that cross examination is ‘beyond any doubt the greatest legal engine ever invented for the discovery of truth,’ one must admit that in the Anglo-American legal system cross examination is the principal means of undermining the credibility of a witness whose testimony is false or inaccurate.”<sup>1</sup> —Justice Stevens

“[C]ross-examination, the most effective tool of the adversary system, is more than a license for lawyers to engage in legitimized hostility. It is a means by which the biases and conflicts of interests of any witness can be surfaced so that the decision maker can see as much as possible of the total picture before arriving at a conclusion.”<sup>2</sup> —David L. Bazelon, Chief Judge, United States Court of Appeals

## I. Introduction

Imagine that you have recently been informed by the defense that they intend to call a psychologist as an expert witness. You start the mad scramble to collect as much information about that expert as you can in the short amount of time you have before he hits the stand. You are fortunate enough to uncover a judicial opinion whereby the sitting judge has stated in a written opinion that “the doctor has abandoned scientific objectivity in order to reach the end he has chosen.” You now continue your search in earnest. You come across another opinion concerning that same expert where the court stated that the doctor “has a checkered history. The Fifth Circuit Court of Appeals was ‘troubled’ with the doctor’s complete inability to explain his irregular methodology, including his failure to ‘report partial conclusions’ that contradicted the findings he submitted to the court.” Yet another court has stated that it found the doctor’s expert testimony “unreliable” and said that he “appears more concerned with legal culpability than with an objective assessment of intellectual capability.” Yet another court states in a published opinion that the federal court found the doctor’s “testimony to be substantial biased and dishonest.” You are now very excited to cross examine the expert, remembering the Supreme Court’s admonishment that “[v]igorous cross-examination . . . [is] the traditional and appropriate means of attacking shaky but admissible evidence.”<sup>3</sup>

But wait a minute. Shortly after you get knee deep in your campaign to discredit the biased expert, the defense files a motion in limine to exclude any evidence of credibility determinations by other courts.<sup>4</sup> The defense wants to do the unthinkable. They want to hire a biased expert with substantial baggage and simultaneously prevent you from bringing that expert’s bias and judicial criticism of his methodology to the attention of the trier of fact.

---

<sup>1</sup> United States v. Salerno, 505 U.S. 317, 328 (1992).

<sup>2</sup> Kenneth Donaldson, *Insanity Inside Out* xi-xii (1<sup>st</sup> ed. 1976).

<sup>3</sup> *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579, 596 (1993).

<sup>4</sup> United States v. Naeem Williams, Case 1:06-cr-00079-JMS-KSC, Doc. 2520 (D. Haw. filed April 3, 2014).

I suggest this precise scenario may be coming soon to a theater near you: your next serious criminal trial. More than ten years ago, United States District Judge Lewis A. Kaplan observed that in “recent years, there has been an explosion in the volume of expert testimony produced at trial.”<sup>5</sup> Judge Kaplan characterized the problem as “The Expert Witness Industry,” and pointed out that the most frequent problem with expert witnesses is their tendency to “abandon objectivity and become advocates for the side that hired them.”<sup>6</sup> More recently, in commenting on the increase in information storage, Google’s Chief Economist said that “Between the dawn of civilization and 2003, we only created five exabytes [of information]; now we’re creating that amount every two days.” The confluence of a dramatic increase in expert testimony and a dramatic increase in information storage means that there may exist a vibrant and extensive record for the many defense experts who frequently testify in criminal trials. Prosecutors should be able to access and use that vibrant record when cross-examining defense experts. Hat in hand with the repeated use of biased “go-to” experts who can reliably be counted upon to advocate favorable opinions from the witness stand, however, will be simultaneous motions to preclude the government from drawing attention to the very fact that makes those witnesses so attractive to defense counsel.

## II. The Seeds of a New Defense Strategy

The genesis of this dual strategy of retaining biased experts and simultaneously moving to exclude any judicial criticism of those same experts can be tracked to *United States v. Northington*.<sup>7</sup> After an *Atkins* retardation hearing in which the prosecution impeached the defense mental health expert with two opinions concerning his prior testimony, the defendant filed a motion in limine seeking to preclude the prosecution from impeaching the expert with those same opinions at trial.<sup>8</sup> Four days later, without the government having filed a response, the trial court granted the motion, but with an interesting caveat.<sup>9</sup> The caveat was that the court felt that the opinions were not impeaching because, although the courts rejected the expert’s conclusions, the same expert would “not be drawing any diagnostic conclusions” in the trial.<sup>10</sup> Accordingly, the court effectively side-stepped the issue of the impeachment use of prior adverse judicial opinions.

Following closely on the heels of *Northington*, the capital defense team followed the same blueprint *with the same expert* in *United States v. Duncan*.<sup>11</sup> In a competency hearing to determine whether the defendant was competent to waive his death penalty appeals, counsel for the defendant presented the testimony of three mental health experts who routinely testify for the defense in capital trials. In a post-hearing brief filed on September 6, 2013, the government brought to the district court’s attention the defense expert bias by stating that “other courts have rejected these defense-retained experts’ opinions in capital cases for several reasons, including bias and lack of credibility,” and cited to seven published cases.<sup>12</sup> The defense fired back and tried to preclude the court from considering the information, stating that “this Court correctly and consistently sustained defendant’s Sixth Amendment confrontation and hearsay objections to repeated attempts by the government to introduce such

---

<sup>5</sup> Lewis A. Kaplan, *Experts in the Courthouse: Problems and Opportunities Remarks at the Milton Handler Antitrust Review* November 29, 2005, 2006 COLUM. BUS. L. REV. 247, 248 (2006).

<sup>6</sup> *Id.* at 249-50, citing Carol Krafka et al, *Judge and Attorney Experiences, Practices, and Concerns Regarding Expert Testimony in Federal Civil Trials*, 8 PSYCHOL. PUB. POL’Y & L. 309, 328 tbl. 6 (2002).

<sup>7</sup> *United States v. Northington*, Case No. 7-550-05, Doc. 1417 (E.D. PA filed May 31, 2013).

<sup>8</sup> *Id.*

<sup>9</sup> *See United States v. Northington*, Case No. 7-550-05, Doc. 1432 (E.D. PA filed June 3, 2013).

<sup>10</sup> *Id.*

<sup>11</sup> *United States v. Duncan*, Case No. 2:07-CR-023-EJL (D. Idaho).

<sup>12</sup> *United States v. Duncan*, Case No. 2:07-CR-023-EJL, Doc. 840 at 15 (D. Idaho).

evidence.”<sup>13</sup> The court punted on the limiting request by the defendant holding that “The Court has not considered that portion of the Government’s brief and, therefore, finds the Defendant’s Motion to be moot.”<sup>14</sup> The court then rejected the defense expert testimony and found the defendant competent to waive his capital appeals.

Next up on the list of cases where the defense has used the same dual strategy was the capital case of *United States v. Naeem Williams*.<sup>15</sup> The defendant’s specific legal strategy was to characterize the prior judicial criticism as “inadmissible hearsay” and as “judicial findings of fact.”<sup>16</sup> Sadly, the defense waited until the day before they were presenting the expert testimony to make an oral and written objection to the expected cross-examination. The government, not having time to adequately respond, agreed not to cross-examine the defense expert with prior judicial determinations that the witnesses’ testimony was not credible, thus mooting the issue.<sup>17</sup>

The next court to consider this new expert legal strategy was the District of Massachusetts. In the federal capital case of *United States v. Sampson*, the defense sought to preclude the government from cross-examining their experts with the credibility determinations of prior courts, largely on the grounds that such evidence is hearsay and would be inappropriate extrinsic evidence.<sup>18</sup> After the government filed its response in opposition, the court denied the motion without prejudice and required any party that wished to cross-examine an expert with the prior judicial determinations to file a motion at least two days prior to the witness’s expected testimony and “identify the specific prior determination the moving party proposes to use” as well as argue why the evidence was not unduly prejudicial.<sup>19</sup>

The dual strategy keeps coming up in current capital litigation. The issue has been briefed in at least one jurisdiction. Additionally, the issue has come up in at least one capital trial and one pre-trial hearing. In both of those cases, the courts allowed cross-examination with prior judicial criticism with some limitations.

### **III. This Cross Has Been Approved—What’s Old is New Again**

Any drama concerning such attempts to prevent prosecutors from impeaching defense experts with court’s prior findings of bias might be more interesting if the precise issue had not been decided by the courts. At least two courts have resolved this precise question in a manner favorable to prosecutors.

In *United States v. Terry*, the Second Circuit specifically endorsed the impeachment that capital defense counsel had tried to prevent.<sup>20</sup> The defendant was charged with narcotics offenses, and the evidence against him included recorded conversations. The defense offered the opinion of a voice expert. In cross-examination, the government questioned the expert about prior occasions where courts criticized the expert and his opinion. The defendant was convicted and appealed. In rejecting the claim that the government improperly impeached his expert, the Second Circuit ruled:

Nor is there any merit in the claim that the prosecutor acted improperly in questioning on cross-examination Harrison’s “voice expert” witness, Louis Gerstman, regarding prior occasions when his testimony in other cases had been criticized by the court as unworthy

---

<sup>13</sup> *United States v. Duncan*, Case No. 2:07-CR-023-EJL, Doc 842 at 2 (D. Idaho).

<sup>14</sup> *United States v. Duncan*, Case No. 2:07-CR-023-EJL, Doc 843 at 8 no.3 (D. Idaho).

<sup>15</sup> *United States v. Naeem Williams*, Case 1:06-cr-00079-JMS-KSC, Doc. 2520 (D. Haw. filed April 3, 2014).

<sup>16</sup> *Id.* at 4.

<sup>17</sup> See transcript of trial *United States v. Naeem Williams*, Case 1:06-cr-00079-JMS-KSC, Doc. 2534 at 7 (D. Haw. filed April 7, 2014).

<sup>18</sup> *United States v. Sampson*, Criminal 1:01-cr-10384, Doc. 2329 (D. Mass. filed July 5, 2016).

<sup>19</sup> *United States v. Sampson*, Criminal 1:01-cr-10384, Doc. 2459 at 64 (D. Mass. filed September 2, 2016).

<sup>20</sup> *United States v. Terry*, 702 F.2d 299, 316 (2d Cir. 1983).

of belief. Proof that a judge of the District of Columbia Superior Court before whom Gerstman had testified as an expert had found that Gerstman had “guessed under oath” was probative of the weight to be accorded to his testimony. FED. R. EVID. 608(b), 613(a).<sup>21</sup>

What is perhaps more amazing, and a more powerful endorsement of the practice, is that *Terry* was decided a full ten years before *Daubert*.

The Court of Criminal Appeals of Alabama also considered the proper scope of cross-examination of a defense expert in a capital murder case in *Albarran v. State* and characterized this particular flavor of cross-examination as “standard fare.”<sup>22</sup> In that case, the defendant claimed that he was retarded and presented expert testimony to that effect. On cross-examination, the prosecutor questioned the expert about the frequency of his testimony in capital-murder cases and about specific capital-murder cases in which he had appeared as an expert. The prosecutor also questioned him about an unpublished order issued by a judge in a Colorado case that was greatly critical of the expert. Then, the prosecutor crossed him with the specific judicial statement:

[Prosecutor]: ‘Dr. Weinstein has chosen the reverse and has abandoned scientific objectivity in order to reach the end he has chosen.’ Were you aware that Judge King had said that about you?<sup>23</sup>

In upholding the extensive cross-examination, the Court held:

“[A]n expert’s testimony in prior cases involving similar issues is a legitimate subject of cross-examination.” *People v. Price*, 1 Cal.4th 324, 457, 3 Cal.Rptr.2d 106, 184, 821 P.2d 610, 688 (1991). “The witness’s personal philosophical opposition to the death penalty is relevant to his credibility.” *People v. Bennett*, 45 Cal.4th 577, 606, 88 Cal.Rptr.3d 131, 156, 199 P.3d 535, 556 (2009). “Wide latitude is permitted in cross-examination to show bias or motive and the affect on a witness’s credibility.” *Bennett v. State*, 933 So.2d 930, 947 (Miss.2006). “The state had the right to question [the expert] about his role as a mitigation expert in other cases to establish a testimonial pattern and thus to expose a possible bias for or against the death penalty.” *State v. Irish*, 807 So.2d 208, 213-14 (La.2002). “We have in fact recognized a host of matters upon which cross-examining counsel may inquire in demonstration of bias, including, for instance, the frequency with which a defense expert testifies for capital defendants.” *Rose v. State*, 787 So.2d 786, 798 (Fla.2001).<sup>24</sup>

The court concluded that “It is clear that the prosecutor’s cross-examination was focused on determining the extent of Dr. Weinstein’s bias against capital punishment.”<sup>25</sup>

#### **IV. A Return to the Scene of the Crime—Defense Counsel on Whose Behalf the Motions Were Filed Agrees that Judicial Criticism is Proper Cross**

Too frequently in our social media age, hypocrisy is captured on video for all the world to see. Such is the case in the latest gambit, sometimes successful, to limit one of a prosecutors most potent weapons against defense professional witnesses: the cross-examination of frequent defense experts with their past court failings. If we rewind the Zapruder film to March, 2015, we can capture defense counsel explaining to an audience of prospective mental health experts that, if they are not careful, future

---

<sup>21</sup> *Id.*

<sup>22</sup> *Albarran v. State*, 96 So. 3d 131, 173 (Ala. Crim. App. 2011).

<sup>23</sup> *Id.* at 172.

<sup>24</sup> *Id.* at 173.

<sup>25</sup> *Id.*

adversaries may cross-examine them with their poorly reasoned or arrived-at expert conclusions. On March 19-21, 2015, John Phillipsborn gave a Keynote Speech to the American Psychology-Law Society in San Diego, California. The title of the speech was “Putting Our Jargon into Your Jargon . . . or, can you help us out?” In that speech, counsel states:

Federal judges have staffs that permit them to do so. They sometimes write very lengthy rulings assessing particular experts. And also as we’re going to find out in one of the later slides, if they feel an expert has undercooked or under-baked his or her particular work they put your name down in a published ruling. That is on the proverbial books that is available to be easily searched through electronic law libraries. *These rulings provide ready fodder for cross-examination*, which is another reason why it makes some degree of sense for you to be very familiar with the rulings that have been issued by particular judges.<sup>26</sup>

This is the self-same defense counsel who appears on the pleadings in the *Naeem Williams* and other cases arguing through co-counsel that this type of impeachment is improper and inappropriate.

## V. Broad Searching Cross-Examination is the Hallmark of Expert Cross-Examination

The heart of the matter is that both parties should be free to engage in searching cross-examination of expert witnesses, especially when those witnesses appear almost exclusively on behalf of one party in a large number of cases. It is axiomatic that the scope of cross-examination is left to the sound discretion of the trial court, and the court of appeals will reverse only for an abuse of discretion.<sup>27</sup> Moreover, improper questioning only rises to the level of reversible error when the misconduct is of sufficient significance to result in the denial of the defendant’s right to a fair trial.<sup>28</sup>

The scope of cross-examination of an expert witness is especially broad. Evidence that is inadmissible on direct examination may be used to test an expert’s credibility, though the court must exercise its discretion to limit the evidence to its proper uses.<sup>29</sup> Wide latitude is afforded in the cross-examination of expert witnesses to test the qualifications, credibility, skill or knowledge, and the value and accuracy of the expert’s opinion.<sup>30</sup> The sources of information used to cross-examine a witness can include hearsay and do not need to be admissible as evidence.<sup>31</sup> The federal rules expressly permit prosecutors to impeach hearsay evidence when that information is offered through experts.<sup>32</sup>

In fact, an expert need not even be aware of the information used to cross-examine them. For example, pursuant to the learned treatise exception to the hearsay rule, an expert may be impeached with a learned treatise if that treatise is established as a reliable authority by a different expert.<sup>33</sup> An expert may also be shown a hearsay report, of which he was unaware, to establish that his opinion is flawed or that he failed to consider information that might change his opinion.<sup>34</sup>

---

<sup>26</sup> See John Philipsborn, *Putting Our Jargon into Your Jargon . . . or, can you help us out?*, <https://www.youtube.com/watch?v=p60UiuuHM1k> (LAST VISITED DEC. 14, 2017).

<sup>27</sup> *United States v. Werme*, 939 F.2d 108, 117 (3d Cir. 1991).

<sup>28</sup> *Greer v. Miller*, 483 U.S. 756, 765 (1987).

<sup>29</sup> *People v. Gonzales*, 253 P.3d 185, 210 (2011).

<sup>30</sup> *State v. Brooks*, 960 S.W.2d 479, 493 (Mo. 1997).

<sup>31</sup> *State v. Dewey*, 86 S.W.3d 434, 439 (Mo. Ct. App. 2002).

<sup>32</sup> FED. R. EVID. 806, see also Fred Warren Bennett, *How to Administer the "Big Hurt" in A Criminal Case: The Life and Times of Federal Rule of Evidence 806*, 44 CATH. U. L. REV. 1135 (1995).

<sup>33</sup> See FED. R. EVID. 803(18)(B).

<sup>34</sup> See *Brooks*, 960 S.W.2d at 492-93.

The Federal Rules of Evidence codify the expanded cross-examination for expert witnesses. FED. R. EVID. 703 permits an expert witness to base his opinion on facts or data which would not be admissible as competent evidence so long as the facts or data are of a type reasonably relied on by experts in the particular field. FED. R. EVID. 705 provides that an expert may be required on cross-examination to disclose the facts or data underlying his opinion, notwithstanding the fact that it is inadmissible hearsay.<sup>35</sup> FED. R. EVID. 806 specifically permits the admission of hearsay to impeach the credibility of any hearsay admitted through the expert. Rule 806 provides:

#### Attacking and Supporting the Declarant's Credibility

When a hearsay statement—or a statement described in Rule 801(d)(2)(C), (D), or (E)—has been admitted in evidence, the declarant's credibility may be attacked, and then supported, by any evidence that would be admissible for those purposes if the declarant had testified as a witness. The court may admit evidence of the declarant's inconsistent statement or conduct, regardless of when it occurred or whether the declarant had an opportunity to explain or deny it. If the party against whom the statement was admitted calls the declarant as a witness, the party may examine the declarant on the statement as if on cross-examination.<sup>36</sup>

FED. R. EVID. 608(b) provides in relevant part:

Specific instances of conduct of a witness for the purpose of attacking . . . his credibility . . . may . . . in the discretion of the court . . . if probative of truthfulness or untruthfulness . . . be inquired into on cross-examination of the . . . witness . . . concerning his character for truthfulness or untruthfulness.

FED. R. EVID. 613(a) provides:

When examining a witness about the witness's prior statement, a party need not show it or disclose its contents to the witness. But the party must, on request, show it or disclose its contents to an adverse party's attorney.<sup>37</sup>

## VI. Giving Teeth to the *Daubert* Directive

The Supreme Court in *Daubert v. Merrell Dow Pharmaceuticals, Inc.* specifically endorsed vigorous and sweeping cross-examination as a way to ferret out “shaky but admissible” expert testimony.<sup>38</sup> Overruling *Frye v. United States*, the Supreme Court expanded the scope of expert testimony potentially admissible at trial by rejecting the “general acceptance” test of *Frye*.<sup>39</sup> The Court specifically addressed the role of cross-examination in challenging questionable or highly contentious expert testimony, stating:

In this regard respondent seems to us to be overly pessimistic about the capabilities of the jury and of the adversary system generally. Vigorous cross-examination, presentation of contrary evidence, and careful instruction on the burden of proof are the traditional and appropriate means of attacking shaky but admissible evidence.<sup>40</sup>

---

<sup>35</sup> See also *United States v. Wright*, 783 F.2d 1091, 1100 (D.C. Cir. 1986) (permitting admission of hearsay statements on cross of expert “for the limited and independent purpose of enabling the jury to scrutinize the expert’s reasoning”).

<sup>36</sup> FED. R. EVID. 806.

<sup>37</sup> FED. R. EVID. 613(a), see also *Terry*, 702 F.2d at 316.

<sup>38</sup> *Daubert*, 509 U.S. at 596.

<sup>39</sup> *Frye v. United States*, 293 F. 1013 (D.C. Cir. 1923).

<sup>40</sup> *Daubert*, 509 U.S. at 596.

The Supreme Court’s support of “vigorous cross” applies with special force to soft scientific evidence like psychology. “Daubert’s adoption of Popper’s view of what constitutes ‘science’ is somewhat problematic for the social sciences in general. Many of the social sciences ‘rely predominately on retrospective observational studies rather than on controlled experimentation, and do not necessarily meet the . . . standard of falsifiability.’”<sup>41</sup>

## VII. The Supreme Court Reverses Cases for Limiting Cross, Not Expanding It

There also exists a clear judicial preference to expand the scope of cross-examination to guarantee adequate opportunity to reveal the biases and deficiencies of witnesses.<sup>42</sup> The Supreme Court’s decision in *Davis v. Alaska*, in which the Supreme Court expanded the scope of cross-examination to include inquiry into juvenile convictions to impeach for bias, is a good example.<sup>43</sup> The Court held, in part:

While counsel was permitted to ask Green *whether* he was biased, counsel was unable to make a record from which to argue *why* Green might have been biased . . . To make such an inquiry effective, defense counsel should have been permitted to expose to the jury the facts from which jurors, as the sole triers of fact and credibility, could appropriately draw inferences relating to the reliability of the witness. Petitioner was thus denied the right of effective cross-examination.<sup>44</sup>

Another example of the Supreme Court’s preference for full and searching cross examination to reveal bias is *United States v. Abel*.<sup>45</sup> In that case, the Supreme Court specifically endorsed the use of collateral and extrinsic evidence. The defendant was on trial for bank robbery and presented evidence through a jail informant that the defendant’s co-conspirator and government witness falsely implicated the defendant to obtain better treatment by the government. The government was then allowed to recall the witness to testify that all three (defendant, government witness, and defense impeaching witness) were part of a “secret type of prison organization” and that one of their gang tenets was to “lie, cheat, and steal” to protect one another. The Ninth Circuit reversed, stating that the evidence was improper impeachment. The Supreme Court reversed, first noting that the Federal Rules of Evidence “do not by their terms deal with impeachment for ‘bias,’ although they do expressly treat impeachment by character evidence and conduct.”<sup>46</sup> The Court went on to state:

Ehle’s testimony about the prison gang certainly made the existence of Mills’ bias towards respondent more probable. Thus it was relevant to support that inference. Bias is a term used in the “common law of evidence” to describe the relationship between a party and a witness which might lead the witness to slant, unconsciously or otherwise, his testimony in favor of or against a party. Bias may be induced by a witness’ like, dislike, or fear of a party, or by the witness’ self-interest. Proof of bias is almost always relevant because the jury, as finder of fact and weigher of credibility, has historically been entitled to assess all evidence which might bear on the accuracy and truth of a witness’ testimony. The “common law of evidence” allowed the showing of bias by extrinsic evidence, while requiring the cross-examiner to “take the answer of the witness” with respect to less favored forms of

---

<sup>41</sup> Henry F. Fradella et. al., *The Impact of Daubert on the Admissibility of Behavioral Science Testimony*, 30 PEPP. L. REV. 403, 412 (2003).

<sup>42</sup> See *United States v. Elliott*, 571 F.2d 880, 908-09 (5th Cir. 1978).

<sup>43</sup> *Davis v. Alaska*, 415 U.S. 308, 318 (1974).

<sup>44</sup> *Id.* (emphasis added).

<sup>45</sup> *United States v. Abel*, 469 U.S. 45 (1984).

<sup>46</sup> *Id.* at 49.

impeachment. See generally McCormick on Evidence, *supra*, § 40, at 89; Hale, Bias as Affecting Credibility, 1 Hastings L. J. 1 (1949).<sup>47</sup>

Consequently, a clear judicial preference exists to expand, not limit, cross-examination, especially when trying to ferret out bias.

## VIII. Courts Themselves Rely upon Prior Court's Credibility Determinations

Courts themselves routinely consider the credibility opinions of other courts when assessing an expert's opinion. For example, in *United States v. Jimenez-Bencevi*,<sup>48</sup> the District Court considered the credibility of capital defense mental health expert Dr. Ricardo Weinstein:

As an expert witness in *Atkins* proceedings, Dr. Weinstein has a checkered history. The Fifth Circuit Court of Appeals was "troubled" with Dr. Weinstein's complete inability to explain his irregular methodology, including his failure to "report partial conclusions" that contradicted the findings he submitted to the court. *Maldonado v. Thaler*, 625 F.3d 229, 239 (5th Cir. 2010). In *Ortiz v. United States*, the district court found Dr. Weinstein's expert testimony "unreliable" and said that he "appears more concerned with legal culpability than with an objective assessment of intellectual capability." *Ortiz v. United States*, 2007 WL 7686126 at \*2-7 (W.D.Mo. Dec. 14, 2007). In *Pizzuto v. Blades*, the district court stated that Dr. Weinstein's findings, at best, were "ambiguous" and that it found it could not "credit" his comprehensive IQ scores. *Pizzuto v. Blades*, 2012 WL 73236 at \*14 (D.Id. Jan. 10, 2012).<sup>49</sup>

In *Ex Parte Moore*,<sup>50</sup> the Court of Criminal Appeals rejected frequent capital defense expert Dr. Stephen Greenspan's opinion stating:

Greenspan acknowledged that, about a year before applicant's hearing, a federal judge issued an opinion in the *Alexis Candelario Santana* case, warning courts across the country to be cautious when reviewing Greenspan's testimony in future intellectual-disability cases. See *United States v. Candelario-Santana*, 916 F.Supp.2d 191, 203-06 (D.P.R. 2013) (finding Greenspan to be "completely lacking in credibility" and stating that due to "bias[]," "considerable careless errors and slipshod disregard for the seriousness of the [court's] inquiry," continued "combative[ness] and evasive[ness] despite being admonished to be more forthcoming with his answers," "unwilling[ness] or [inability] to explain evidence that tended to refute his conclusions[,] and . . . little explanation . . . as to why he thought the government's experts' assessments were incorrect," Greenspan's testimony in an *Atkins* evidentiary hearing "suffered from extreme deficits" such that it "was fundamentally unreliable" and should be disregarded).<sup>51</sup>

Accordingly, it seems odd to suggest that courts can and should rely upon prior judicial criticism in assessing the reliability and bias of experts, but that same information should be denied to jurors who are asked to make the very same crucial credibility determinations.

---

<sup>47</sup> *Id.* at 52.

<sup>48</sup> *United States v. Jimenez-Bencevi*, 934 F. Supp. 2d 360 (D.P.R. 2013).

<sup>49</sup> *Id.* at no.2.

<sup>50</sup> *Ex Parte Moore*, 470 S.W.3d 481 (Tex. Crim. App. 2015).

<sup>51</sup> *Id.* at no.33.

## IX. Back to Basics

In this increasingly commercialized world of expert witnesses, broad cross-examination to establish expert bias should be the rule, not the exception. The search for prior judicial decisions critical of defense, and prosecution, experts should be a prosecutor's first step in preparing for the examination of expert witnesses. Of course, the prescription advocated here to impeach experts with prior adverse judicial findings applies with equal force to the government as well. Prosecutors should thoroughly research their own potential experts before retaining them. When appropriate, the government should file *Daubert* motions to preclude the testimony outright. Assuming that identified expert transgressions do not rise to the level of judicial exclusion, prosecutors should be aware that lingering in the wings is a defense motion to preclude the government from cross-examining experts about their prior judicial criticism. Perhaps a preemptive motion in limine to bring to the court's attention the previous judicial criticism is appropriate.

### ABOUT THE AUTHOR

□ **James D. Peterson** is a trial attorney in the Capital Case Section, providing litigation and trial assistance and expertise to local United States Attorney's Offices that are prosecuting death penalty cases. Jim has been with the Department of Justice in the Capital Case Section since 2012. Prior to joining CCS, Jim was a state prosecutor in Virginia for over eighteen years. During that time, he tried more than 130 jury trials, including multiple capital murder cases. Jim is a past recipient of the Warren Von Schuch Award for outstanding Virginia prosecutor. He has lectured throughout the country on subjects relating to computer crimes, the insanity defense, capital case litigation, as well as mental health issues in criminal trials. Prior to becoming a prosecutor, Jim practiced commercial litigation in Dallas, Texas and Washington D.C. for several years. Jim graduated from Franklin and Marshall College in Lancaster, Pennsylvania and from Syracuse University College of Law, summa cum laude. At Syracuse, Jim was a member of the Law Review. He is married with two children.

Page Intentionally Left Blank

# Two New Self-Authentication Rules That Make It Easier to Admit Electronic Evidence

*John M. Haried*

*Criminal eDiscovery Coordinator*

*Executive Office for United States Attorneys*

## I. Introduction

Authenticating evidence can make or break a trial. Due to the proliferation of computers, cell phones, and social media into everyday life, trial lawyers now focus a lot of their energy, time, and worry on authenticating electronic evidence.<sup>1</sup> To address that situation, the Federal Rules of Evidence now includes two new rules that allow self-authentication of electronic machine-generated evidence. The rules are effective as of December 1, 2017. They can save time and money by creating a pretrial procedure for the parties to eliminate live, in-court testimony from mere authentication witnesses when there is not a genuine dispute about authenticity.

## II. The Problem: Unproductive Roadblocks to Authentication of Electronic Evidence

In June 2013, Pfc. Bradley Manning was facing a military court-martial on charges of leaking classified information to WikiLeaks. The court-martial was conducted at Fort Meade, Maryland, under the Military Rules of Evidence, which follow the Federal Rules of Evidence.

The prosecution argued that WikiLeaks had posted on its website a solicitation for the types of classified information that Manning was charged with providing. As evidence, the prosecutor sought to introduce Exhibit 109, a screen capture of WikiLeaks' "Most Wanted Leaks of 2009." The prosecution obtained Exhibit 109 from Archive.org, located in San Francisco, which operates the Wayback Machine.<sup>2</sup> The Wayback Machine is an internet archiving system that uses software programs known as web crawlers to surf the internet and automatically capture and store images from webpages.

Manning objected to Exhibit 109 as hearsay. In ruling on authentication during trial, the judge found that Exhibit 109 was not a business record that could be self-authenticated under FED. R. EVID. 902(11). However, the trial judge ruled that Exhibit 109 was relevant and admissible if the prosecution brought the custodian of records from San Francisco to Maryland to provide live testimony to authenticate it on other Rule 901 grounds. As the witness was about to depart San Francisco for Maryland, the defendant stipulated to the authenticity of Exhibit 109.

The Manning case illustrates several issues common to authentication of electronic machine generated information. First, in today's electronic information world, authentication witnesses often live

---

<sup>1</sup> Two excellent resources on authentication of many types of electronic evidence are Hon. Paul W. Grimm, Daniel J. Capra, and Gregory P. Joseph, *Authenticating Digital Evidence*, 69 BAYLOR L.REV. 1 (2017); Hon. Paul W. Grimm et. al., *Back to the Future: Lorraine v. Markel American Insurance Co. and New Findings on the Admissibility of Electronically Stored Information*, 42 AKRON L. REV. 357 (2009).

<sup>2</sup> Internet Archive: Wayback Machine, <http://archive.org/web/> (LAST VISITED DEC. 1, 2017).

far from the courthouse, so presenting live testimony is expensive. The records of Archive.org, Google, Facebook, Microsoft, and other custodians of pervasive electronic records may be evidence in any courthouse in the nation. Second, many categories of machine-generated information are not business records because the custodian did not create the record's content or rely upon the content's accuracy to conduct its business. Third, while the party against whom the evidence is offered often does not genuinely dispute the authenticity of the item, he can force the exhibit's proponent to undertake great trouble and expense because the evidence rules—until now—did not provide a mechanism to resolve the authentication issues before trial. Because machine-generated electronic information is a growing source of important evidence, litigants need a mechanism to avoid unnecessary authentication disputes that waste their money and the court's time.

### III. The Solution: New Rules 902(13) and 902(14)

Effective December 1, 2017, new Rules 902(13) and 902(14) will provide a mechanism for parties to identify and address authentication issues for evidence generated by an electronic process or system. The new rules combine the conceptual frameworks of Rule 901(b)(9)—authentication by evidence describing a process or system that produces an accurate result—and Rules 902(11) and (12)—self-authentication of business records:

#### Rule 902. Evidence That Is Self-Authenticating

The following items of evidence are self-authenticating; they require no extrinsic evidence of authenticity in order to be admitted:

\* \* \*

(13) *Certified Records Generated by an Electronic Process or System.* A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11). (See Sidebar on Page 129 for Committee Notes [1]).

\* \* \*

(14) *Certified Data Copied from an Electronic Device, Storage Medium, or File.* Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent also must meet the notice requirements of Rule 902(11). (See Sidebar on Page 136 for Committee Notes [2]).

### IV. Illustrative Use Cases

The following hypotheticals illustrate how litigators can use new Rules 902(13) and 902(14) to authenticate electronic evidence, eliminate unnecessary witnesses, and save time and money.

Example One: *Proving that a particular USB device was connected to (i.e., plugged into) a computer.* In a civil case litigated in Chicago, a disputed issue is whether Susan Hall used her personal computer to access files stored on a particular USB thumb drive. Her computer uses the Windows operating system, which automatically records information about every USB device connected to her computer in a database known as the “Windows registry.” The Windows registry database is maintained on the computer by the Windows operating system to facilitate the computer's operations. The registry logs the computer's operations and users' actions, for example, when a user accessed particular files or applications such as internet browsers. A forensic technician, located near Hall's home in Boston, has provided a printout from the Windows registry that indicates that a USB thumb drive, identified by

manufacturer, model, and serial number, was last connected to Ms. Hall's computer at a specific date and time.

Without Rule 902(13), the proponent of the evidence would need to present testimony from the forensic technician who obtained the printout in order to establish the authenticity of the evidence. During testimony, the forensic technician typically would be asked to testify about his or her background and qualifications, the process used to conduct the digital forensic examinations, the process by which the Windows operating system maintains information in the Windows registry, including information about USB devices connected to the computer, and the steps taken to examine the Windows registry and to produce the printout identifying the USB device.

With Rule 902(13), the proponent of the evidence could obtain a written certification from the forensic technician, stating that the Windows operating system regularly records information in the Windows registry about USB devices connected to a computer, that the process by which such information is recorded produces an accurate result, and that the printout accurately reflected information stored in the Windows registry of Hall's

computer. The proponent would be required to provide reasonable written notice of its intent to offer the printout as an exhibit and to make the written certification and proposed exhibit available for inspection. If the adversary did not dispute the accuracy or reliability of the process that produced the exhibit, the proponent would not need to call the forensic technician as a witness to establish the authenticity of the

#### COMMITTEE NOTE [1]

The amendment sets forth a procedure by which parties can authenticate certain electronic evidence other than through the testimony of a foundation witness. As with the provisions on business records in Rules 902(11) and (12), the Committee has found that the expense and inconvenience of producing a witness to authenticate an item of electronic evidence is often unnecessary. It is often the case that a party goes to the expense of producing an authentication witness and then the adversary either stipulates authenticity before the witness is called or fails to challenge the authentication testimony once it is presented. The amendment provides a procedure under which the parties can determine in advance of trial whether a real challenge to authenticity will be made, and can then plan accordingly.

Nothing in the amendment is intended to limit a party from establishing authenticity of electronic evidence on any ground provided in these Rules, including through judicial notice where appropriate.

A proponent establishing authenticity under this Rule must present a certification containing information that would be sufficient to establish authenticity were that information provided by a witness at trial. If the certification provides information that would be insufficient to authenticate the record if the certifying person testified, then authenticity is not established under this Rule. The Rule specifically allows the authenticity foundation that satisfies Rule 901(b)(9) to be established by a certification rather than the testimony of a live witness.

The reference to the "certification requirements of Rule 902(11) or (12)" is only to the procedural requirements for a valid certification. There is no intent to require, or permit, a certification under this rule to prove the requirements of Rule 803(6). Rule 902(13) is solely limited to authentication, and any attempt to satisfy a hearsay exception must be made independently.

A certification under this Rule can establish only that the proffered item has satisfied the admissibility requirements for authenticity. The opponent remains free to object to admissibility of the proffered item on other grounds—including hearsay, relevance, or in criminal cases the right to confrontation. For example, assume that a plaintiff in a defamation case offers what purports to be a printout of a webpage on which a defamatory statement was made. Plaintiff offers a certification under this Rule in which a qualified person describes the process by which the webpage was retrieved. Even if that certification sufficiently establishes that the webpage is authentic, defendant remains free to object that the statement on the webpage was not placed there by defendant. Similarly, a certification authenticating a computer output, such as a spreadsheet, does not preclude an objection that the information produced is unreliable—the authentication establishes only that the output came from the computer.

A challenge to the authenticity of electronic evidence may require technical information about the system or process at issue, including possibly retaining a forensic technical expert; such factors will affect whether the opponent has a fair opportunity to challenge the evidence given the notice provided.

The reference to Rule 902(12) is intended to cover certifications that are made in a foreign country.

exhibit.<sup>3</sup> The court would make the threshold Rule 104(a) authenticity finding and admit the exhibit, absent other proper objections.

*Example Two: Proving that a server was used to connect to a particular web page.* A malicious hacker executed a denial-of-service attack against Acme’s website. Acme’s web server maintained an Internet Information Services (IIS) log that automatically records information about every internet connection routed to the web server to view a web page, including the IP address, web page, user agent string, and what was requested from the website. The IIS logs reflected repeated access to Acme’s website from an IP address known to be used by the hacker. The proponent wants to introduce the IIS log to prove that the hacker’s IP address was an instrument of the attack.

Without Rule 902(13), the proponent would have to call a website expert to testify about the server’s operating system, his search of the IIS log, how the IIS log works, and that the exhibit is an accurate record of the IIS log.

With Rule 902(13), the proponent would obtain a website expert’s certification of the facts establishing authenticity of the IIS log and provide the certification and exhibit to the opposing party with reasonable notice that it intends to offer the exhibit at trial. If the opposing party does not timely dispute the reliability of the process that produced the IIS log, then the proponent would not need to call the website expert to establish authenticity.

*Example Three: Proving that a person was or was not near the scene of an event.* Robert Jackson is a defendant in a civil action alleging that he was the driver in a hit-and-run collision with a U.S. Postal Service mail carrier in Atlanta at 2:15 p.m. on March 6, 2016. Mr. Jackson owns an iPhone, which has software that records machine-generated dates, times, and GPS coordinates of each picture he takes with his iPhone. Mr. Jackson’s iPhone contains two pictures of his home in an Atlanta suburb at about 1 p.m. on March 6. He wants to introduce into evidence the photos recovered forensically from his iPhone, together with the metadata, including the date, time, and GPS coordinates, to corroborate his alibi that he was at home several miles from the scene at the time of the collision.

Without Rule 902(13), the proponent would have to call the forensic technician to testify about Jackson’s iPhone’s operating system, his search of the phone, how the metadata was created and stored with each photograph, and that the exhibit is an accurate record of the photographs.

With Rule 902(13), the proponent would obtain the forensic technician’s certification of the facts establishing authenticity of the exhibits and provide the certification and exhibits to the opposing party with reasonable notice that it intends to offer the exhibits at trial. If the opposing party does not timely dispute the reliability of the process that produced the iPhone’s photos and their metadata, then the proponent would not have to call the technician to establish authenticity.

*Example Four: Proving association and activity between alleged co-conspirators.* Ian Nicholas is charged with conspiracy to rob the First National Bank in San Diego on January 30, 2016. Two armed robbers drove away in a silver Ford Taurus. Dain Miller is the alleged co-conspirator. Dain was arrested on an outstanding warrant on February 1, 2016, and in his pocket was his Samsung Galaxy phone. The phone’s software automatically maintained a log of text messages that includes the text content, date, time, and number of the other phone involved. Pursuant to a warrant, forensic technicians examined Dain’s phone and located four text messages to Ian’s phone from January 29: “Meet my house @9”; “Is Taurus the Bull out of shop?”; “Sheri says you have some blow”; and “see u tomorrow.” At Ian’s trial the government wants to offer the four text messages to prove the conspiracy.

---

<sup>3</sup> There are many other examples of the same types of machine-generated information built into computer operating systems, for example, internet browser histories and Wi-Fi network access logs.

Without Rule 902(13), the proponent would have to call the forensic technician to testify about Dain's phone's operating system, his search of the phone's text message log, how the log was created, and that the exhibit is an accurate record of the phone's log.

With Rule 902(13), the proponent would obtain the forensic technician's certification of the facts establishing authenticity of the exhibit and provide the certification and exhibit to the opposing party with reasonable notice that it intends to offer the exhibit at trial. If the opposing party does not timely dispute the reliability of the process that produced the phone's log, then the court would make an authenticity finding and admit the exhibit.

It is important to differentiate authentication from admissibility. New Rules 902(13) and 902(14) do not address admissibility issues, such as hearsay. As discussed below, under Rule 902(13), the adversary—here, defendant Ian—would retain his hearsay objections to the text messages found on Dain's phone.

*Example Five: Using Rule 902(14) to authenticate a copy.* In the armed robbery scenario, Example Four above, forensic technician Smith made a forensic copy of Dain's Samsung Galaxy phone in the field in San Diego. Smith verified that the forensic copy was identical to the original phone's text logs using an industry standard methodology (e.g., hash value or other means). Smith then sent the copy to forensic technician Jones, who performed his examination at his lab in Atlanta. Jones used the copy to conduct his entire forensic examination so that he would not inadvertently alter the data on the phone. Jones found the text messages. The government wants to offer the copy into evidence as part of the basis for Jones' testimony about the text messages he found.

Without Rule 902(14), the government would have to call two witnesses. First, forensic technician Smith would need to testify about making the forensic copy of information from Dain's phone, and about the methodology that he used to verify that the copy was an exact copy of information inside the phone. Second, the government would have to call forensic technician Jones to testify about his examination.

With Rule 902(14), the government would obtain Smith's certification of the facts establishing how he copied the phone's information and then verified the copy was true and accurate. Before trial the government would provide the certification and exhibit to the opposing party—here, defendant Ian—with reasonable notice that it intends to offer the exhibit at trial. If Ian's attorney does not timely dispute the reliability of the process that produced the Samsung Galaxy's text message logs, then the government would only call forensic technician Jones. Depending upon its trial strategy, the government might also seek to authenticate the text message logs under Rule 902(13).

## **V. Potential Issues with the Application of Rule 902(13)**

Electronic evidence comes from many sources, thereby implicating different rules of evidence. In criminal cases, electronic evidence—like SMS text messages or photos—can come directly from the memory of personal cell phones and computers seized during an arrest or pursuant to a search warrant. Usually the business records rules—Rules 803(6) and 902(11)—do not apply to information found on personal devices. Conversely, the business records rules often apply to electronic evidence in the records of commercial service providers obtained by subpoena or other legal process. Internet service providers (ISPs) offer a wide array of services, including internet access, mailboxes, and data hosting. The ranks of ISPs include AT&T, DISH Network, Time Warner, Comcast, Century Link, Verizon, and many others. ISPs' business records include machine-generated information like the date and time stamps, accounts used, and routing histories. However, other information maintained by ISPs does not qualify as a business record because the ISP does not rely upon the truthfulness or accuracy of the information to conduct its business. In civil cases, electronic evidence can come from those sources or from the parties' own computer systems. Below are issues to consider.

## A. Hearsay Contained Within Machine-Generated Electronic Information

Machine-generated information is not hearsay because it is not a “statement” of a “person” under Rule 801(a).<sup>4</sup> In Example One above, the Windows registry for Susan Hall’s home computer contained only machine-generated data about the computer’s operations and users’ actions, such as when a thumb drive was connected to the computer, when a user opened an internet browser, or when the computer was connected to a particular wireless network. That information is not hearsay. Similarly, in Example Three, the record of the date, time, and GPS coordinates for pictures taken on Robert Jackson’s iPhone contained no hearsay.

However, other categories of machine-generated electronic information contain both nonhearsay information and hearsay statements. Rule 902(13) is limited; it only serves as a mechanism to authenticate the machine-generated information, not the hearsay statement. For example, in these text messages found in the memory of Individual B’s cell phone, there is a hearsay statement implicating Dan Defendant:

Individual A, Friday at 9:50 am: “Who shot the bank guard?”

Individual B, Friday at 9:52 am: “Not me. Last week Tammy told me she saw Dan shoot him.”

At the trial of Dan Defendant, the prosecution could authenticate only some portions of the text messages found on Individual B’s phone by a certification from a forensic technician pursuant to Rule 902(13)—such as which phones were used and the date and times of the text messages. However, the text messages would not be admitted as evidence on that basis alone because Dan Defendant would retain his hearsay objection to the statement by Tammy that she saw Dan shoot the bank guard. The Committee Note to Rule 902(13) notes that the adversary retains other objections, like hearsay.

The result would be the same if the prosecution subpoenaed the very same text messages from the ISP’s records. The prosecution could authenticate portions of the messages with the ISP’s certification under either Rule 902(11) or 902(13)—like the date and time stamps and accounts used—but under either rule, Defendant would still retain his hearsay objection. Moreover, as discussed below, neither Rule 902(11) nor Rule 902(13) alone would provide the prosecution a basis to overcome an objection to the text message’s hearsay content.

## B. The Interplay Between Hearsay, Business Records, and Rules 803(6), 902(11), and 902(13)

As seen, many instances will arise where the rules governing the admissibility and authentication of electronic evidence intersect and overlap. Some common examples are Facebook posts, instant message chats, emails, and text messages where the evidence of the communication comes from the records of a commercial service provider like Facebook, Instagram, Google, Microsoft, or Verizon. Some facets of the record of a Facebook post, an email, or a text message are machine-generated, such as the date and time stamp and the source and destination account. Other facets, like the message’s content, may be admissible or inadmissible hearsay statements.

Recently, the Third Circuit addressed these issues and the resulting business records authentication requirements under Rules 803(6) and 902(11). In *United States v. Browne*,<sup>5</sup> the criminal charges included enticement of minors to engage in sexual activity, and the disputed evidence was a series of Facebook chats between the defendant and three victims. The government argued that the Facebook chats in their entirety were Rule 803(6) business records that could be self-authenticated under

<sup>4</sup> See, e.g., *United States v. Lizarraga-Tirado*, 789 F.3d 1107, 1109-10 (9th Cir. 2015) (finding Google Earth satellite images and stamped coordinates not statements of people); *United States v. Lamons*, 532 F.3d 1251, 1261-65 (11th Cir. 2008) (determining Sprint billing and call report data not statements of people).

<sup>5</sup> *United States v. Browne*, 834 F.3d 403, 405 (3d Cir. 2016).

Rule 902(11). The court disagreed, holding that Facebook chats contained a mixture of Facebook’s business records and nonbusiness record information. The business record elements were limited to “certain aspects of the communications exchanged over that platform, that is, confirmation that the depicted communications took place between certain Facebook accounts, on particular dates, or at particular times.”<sup>6</sup> The court held that the content of the communications between the defendant and victims were not business records because Facebook did not verify or rely upon the substance of the chats in the course of its business. The chats were merely sent via the Facebook platform.<sup>7</sup>

New Rule 902(13) adds an alternative mechanism of authenticating Facebook chats like those in *Browne*, but it does not change the outcome. Facebook chats—and other electronic evidence—may be authentic because they are the product of a system or process that produces an accurate result. However, portions of the record may be inadmissible because the adversary has other valid evidentiary objections, such as hearsay. In the Facebook chat example, a Rule 902(13) certification could establish that the Facebook system accurately records the substance of the chats exchanged, but the certification would not preclude a hearsay or other appropriate objection to the chats’ content.

It bears noting that for some types of electronic evidence, the proponent cannot simply rely upon a Rule 902(13) certification to establish fully the authentication required by Rule 901(a). The proponent may need to further authenticate the evidence by linking it to a particular individual to establish authorship. In *Browne*, the court faced this issue because the defendant claimed that the government’s evidence was insufficient to link him to the Facebook account of “Billy Button.” The court recited the direct and circumstantial evidence linking the defendant to the account: He told the police it was his account; the victims testified to meeting the defendant in person, identified him, and described their chat communications; and a cell phone the defendant used to contact the victims was found at the defendant’s home. In finding the totality of the government’s evidence sufficient to tie the defendant to the “Billy Button” account, the court held that it is “no less proper to consider a wide range of evidence for the authentication of social media records than it is for more traditional documentary evidence.”<sup>8</sup>

### **C. Confrontation Clause Limitations on Self-Authentication in Criminal Cases**

In criminal cases, there are constitutional limitations on what evidence can be self-authenticated. The Advisory Committee on Evidence Rules carefully considered the Confrontation Clause issues during adoption of Rules 902(13) and 902(14). Relying upon the precedent for Rule 902(11) certificates, the Advisory Committee concluded that Rule 902(13) would not violate the Confrontation Clause because the certificate only authenticates the electronic record.<sup>9</sup>

For example, in *United States v. Yeley-Davis*, the Tenth Circuit Court of Appeals held that a Rule 902(11) certificate authenticating phone records as business records was properly admitted over the defendant’s confrontation objection:

“Justice Scalia expressly described the difference between an affidavit created to provide evidence against a defendant and an affidavit created to authenticate an admissible record . . . . In addition, Justice Scalia rejected the dissent’s concern that the majority’s holding would disrupt the long-accepted practice of authenticating documents under Rule 902(11) and would call into question the holding in *Ellis* [a case which had rejected a Confrontation Clause challenge to the use of Rule 902(11)]. See *Melendez-Diaz*, 129 S.Ct. at 2532 n. 1 (“Contrary to the dissent’s suggestion, . . . we do not hold, and it is not the case, that anyone

---

<sup>6</sup> *Id.* at 411.

<sup>7</sup> *Id.* at 410-11.

<sup>8</sup> *Id.* at 412.

<sup>9</sup> Advisory Committee on Evidence Rules, 26-27 (Apr. 29).

whose testimony may be relevant in establishing the . . . authenticity of the sample . . . must appear in person as part of the prosecution's case.”).<sup>10</sup>

Other circuits applying the *Melendez-Diaz* carve-out have held that authentication certificates do not violate the Confrontation Clause.

Electronic information resulting from a process or system that produces an accurate result is not hearsay because it is not *testimonial* under *Melendez-Diaz*; the machine is not a “person,” and machine-generated information is not a “statement” under Rule 801(a).<sup>11</sup> Similarly, the fact that machine-generated information was prepared in anticipation of litigation is not a bar to its admissibility because, unlike the lab chemist’s affidavit in *Melendez-Diaz*, machine-generated information is not *testimonial*. However, any additional information in the form of witness testimony that interprets or explains the result may indeed be *testimonial*. Thus, a properly constructed certificate does not violate the Confrontation Clause. Obviously, certificates deserve careful drafting by lawyers and scrutiny by trial judges.

#### **D. Limitations on What Self-Authentication Certificates Can Accomplish**

Whether in criminal or civil cases, Rule 902(13) certifications should be limited to authenticating the accuracy of the machine-generated *result*. They should not become a Trojan horse for providing the fact-finder with additional information in the form of a witness’s interpretation or explanation of the resulting evidence.

To illustrate, consider a criminal case where the prosecution obtains a Rule 902(13) certification for a Drug Enforcement Administration lab report of a gas chromatograph test that reports a positive result for heroin and an affidavit of a lab chemist stating that, in his opinion, the sample contained heroin. The defendant makes several objections to the prosecution’s evidence: The gas chromatograph report is not authentic and is hearsay, the lab chemist’s opinion is hearsay, both reports violate the Confrontation Clause and are inadmissible because they were prepared in anticipation of litigation, and the Rule 902(13) certification itself is inadmissible hearsay that violates the Confrontation Clause. We will consider each in turn.

The gas chromatograph’s machine-generated report of the result, authenticated by an appropriate Rule 902(13) certification, is admissible. It is not *testimonial*—and not hearsay—because it is not a “statement” of a “person.” For the same reason, the fact that the report was prepared in anticipation of litigation is not a bar to its admissibility.

In contrast, the lab chemist’s affidavit is hearsay and its admission would violate the Confrontation Clause. The court held in *Melendez-Diaz* that extra-judicial statements contained in *testimonial* materials, such as affidavits, depositions, prior testimony or confessions, require live testimony from the witness.

The court may consider the Rule 902(13) certificate for the limited purpose of the Rule 104(a) threshold determination of admissibility, and the court can make the certificate part of the trial record.<sup>12</sup>

---

<sup>10</sup> *United States v. Yeley-Davis*, 632 F.3d 673, 680-81 (10th Cir. 2011).

<sup>11</sup> *See, e.g., United States v. Moon*, 512 F.3d 359, 362 (7th Cir. 2008) (determining that readings from an infrared spectrometer and a gas chromatograph did not violate *Crawford* because “data are not ‘statements’ in any useful sense. Nor is a machine a ‘witness against’ anyone.”).

<sup>12</sup> *See, e.g., United States v. Albino-Loe*, 747 F.3d 1206, 1211 (9th Cir. 2014) (finding no confrontation violation where the “certifications at issue here did not accomplish anything other than authenticating the A-File documents to which they were attached. In particular, they did not explicitly state anything about Albino-Loe’s alienage.”); *United States v. Brinson*, 772 F.3d 1314, 1322-23 (10th Cir. 2014) (“The prosecution presented the certificate in part to authenticate the debit card records under Federal Rule of Evidence 902(11). This rule “permits a party to establish

Trial lawyers know that several strategies are in play when devising the right mixture of exhibits and witness testimony. On the one hand, the report of the result, even coupled with the authenticity certificate, may fail to provide sufficient context and explanation of the result to be persuasive and memorable for the jury. Thus, a trial attorney might eliminate one or more purely authentication witnesses by utilizing Rule 902(13), but still call a competent witness to provide explanation and context for the result. On the other hand, if the result is either self-explanatory, not central to the case, not seriously disputed by the opposing party, or not contested by the opposing party, then the trial lawyer may conclude that the report of the result standing alone is sufficient. Thus, different trial strategies will lead lawyers to use Rule 902(13) in various ways.

## **E. Addressing Allegations of Tampering with Electronic Evidence**

The speculative possibility that electronic evidence could be falsified or tampered with clearly is not a sufficient basis for an objection to authenticity.<sup>13</sup>

However, when there are credible grounds to suspect tampering, Rule 902(13) can provide a mechanism to address them. For example, in a civil personal-injury case, plaintiff Moreno claims she suffered serious injuries to her legs from the defendant's conduct. The defendant wants to use a photograph of Moreno dancing with friends to disprove the claimed injuries; the photo's date stamp is just a few weeks after Moreno's injuries. The photo was recovered from the cell phone of Moreno's ex-husband. Moreno denies being at the photo's location on that date, and she asserts someone used Photoshop software to put her image into the photo. How does Rule 902(13) help address this issue?

The defendant may elect to utilize Rule 902(13) to authenticate the photo, in whole or in part. Because Rule 902(13) incorporates the "reasonable written notice" provisions of Rule 902(11), before the trial the defendant must give Moreno written notice of his intent to use the photo and the basis for authenticating the photo. Under Rule 902(13), Moreno has the right to challenge the prosecution's basis for authentication. From the defendant's written notice, the court and Moreno will have a better understanding of which authentication factors are not disputed and which are disputed. It may be that Moreno does not dispute the manner in which the electronic file of the photo was collected from the phone, at which point the defendant can eliminate that authentication witness by using a certificate. If tampering via Photoshop is Moreno's real challenge to authenticity, then the pretrial self-authentication process will help focus the parties' dispute. Alternatively, if the defendant did not invoke Rule 902(13) before trial, then the defendant would need to call all of its authentication witnesses at trial, and Moreno would make her tampering challenge at trial.

---

the authenticity of documents as domestic business records through a declaration from the records' custodian." *quoting* United States v. Lewis, 594 F.3d 1270, 1278 (10th Cir.2010) . . . Mr. Brinson relies on *Melendez-Diaz v. Massachusetts* . . . There, the Supreme Court held that affidavits showing the results of a forensic analysis are testimonial statements . . . *Melendez-Diaz* does not apply. Our certificate does not contain any "analysis" that would constitute out-of-court testimony. Without that analysis, the certificate is simply a non-testimonial statement of authenticity." See also *Yeley-Davis*, 632 F.3d at 681 ("The Court's ruling in *Melendez-Diaz* does not change our holding that Rule 902(11) certifications of authenticity are not testimonial.").

<sup>13</sup> *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 573 (D. Md. 2007) ("The possibility of alteration does not and cannot be the basis for excluding e-mails as unidentified or unauthenticated as a matter of course." *quoting* United States v. Safavian, 435 F.Supp.2d 36, 41 (D.D.C.2006)).

## VI. Rule 902(14)

Rule 902(14) provides litigants a mechanism to eliminate what is usually perfunctory and uncontested testimony about copying data. Often, data is copied from an original storage medium—for example, the memory of a computer or cell phone—in order to conduct a forensic examination without altering the contents or metadata of the original device. To preserve the original, almost all forensic examinations are conducted on copies.

The software tools for verifying that the copy matches the original include several industry-standard programs. New software and methodologies are coming into the market. Rule 902(14) is designed to adapt to technology as it evolves.

Rule 902(14) is simple and straightforward. By providing a mechanism for the parties to address any authentication issues before trial, it should enable the parties to eliminate unnecessary authentication witnesses and save time and money.

## VII. Conclusion

New Rules 902(13) and 902(14) provide litigants with a pretrial procedure to assess whether they have a genuine dispute about the authenticity of records of results generated by an electronic process or system that produces an accurate result.

Many types of computer-generated information are routinely relied upon in daily life because they are trustworthy. However, the witnesses who can authenticate electronic evidence are spread across the globe, and getting them to the courthouse is one of the expensive complications that make going to trial unaffordable for many litigants. Where there is not a genuine dispute about the authenticity of such

### COMMITTEE NOTE [2]

The amendment sets forth a procedure by which parties can authenticate data copied from an electronic device, storage medium, or an electronic file, other than through the testimony of a foundation witness. As with the provisions on business records in Rules 902(11) and (12), the Committee has found that the expense and inconvenience of producing an authenticating witness for this evidence is often unnecessary. It is often the case that a party goes to the expense of producing an authentication witness, and then the adversary either stipulates authenticity before the witness is called or fails to challenge the authentication testimony once it is presented. The amendment provides a procedure in which the parties can determine in advance of trial whether a real challenge to authenticity will be made, and can then plan accordingly.

Today, data copied from electronic devices, storage media, and electronic files are ordinarily authenticated by “hash value.” A hash value is a number that is often represented as a sequence of characters and is produced by an algorithm based upon the digital contents of a drive, medium, or file. If the hash values for the original and copy are different, then the copy is not identical to the original. If the hash values for the original and copy are the same, it is highly improbable that the original and copy are not identical. Thus, identical hash values for the original and copy reliably attest to the fact that they are exact duplicates. This amendment allows self-authentication by a certification of a qualified person that she checked the hash value of the proffered item and that it was identical to the original. The rule is flexible enough to allow certifications through processes other than comparison of hash value, including by other reliable means of identification provided by future technology.

Nothing in the amendment is intended to limit a party from establishing authenticity of electronic evidence on any ground provided in these Rules, including through judicial notice where appropriate.

A proponent establishing authenticity under this Rule must present a certification containing information that would be sufficient to establish authenticity were that information provided by a witness at trial. If the certification provides information that would be insufficient to authenticate the record if the certifying person testified, then authenticity is not established under this Rule.

The reference to the “certification requirements of Rule 902(11) or (12)” is only to the procedural requirements for a valid certification. There is no intent to require, or permit, a certification under this Rule to prove the requirements of Rule 803(6). Rule 902(14) is solely limited to authentication, and any attempt to satisfy a hearsay exception must be made independently.

A certification under this Rule can only establish that the proffered item is authentic. The opponent remains free to object to admissibility of the proffered item on other grounds—including hearsay, relevance, or in criminal cases the right to confrontation. For example, in a criminal case in which data copied from a hard drive is proffered, the defendant can still challenge hearsay found in the hard drive, and can still challenge whether the information on the hard drive was placed there by the defendant.

A challenge to the authenticity of electronic evidence may require technical information about the system or process at issue, including possibly retaining a forensic technical expert; such factors will affect whether the opponent has a fair opportunity to challenge the evidence given the notice provided.

The reference to Rule 902(12) is intended to cover certifications that are made in a foreign country.

information, these new rules provide litigants with the tools to eliminate uncontested authentication witnesses, focus on the real issues in contention, and save time and money.

#### **ABOUT THE AUTHOR**

□ **John M. Haried** is the Criminal eDiscovery Coordinator for the Executive Office for United States Attorneys (EOUSA) in the Department of Justice. He has been an Assistant United States Attorney in Colorado for 27 years. He is a member of EOUSA's eLitigation Working Group. He is an instructor for the Office of Legal Education at the National Advocacy Center on electronic management of case information and discovery-related topics. He previously wrote for the US Attorney Bulletin: USAO Options for Managing Small, Medium, and Large Cases (2016); The New Criminal ESI Discovery Protocol (2012); Flying Cars and Web Glasses: How the Digital Revolution is Changing Law Enforcement (2011).

*This article is republished here with the permission of Judicature.*

Page Intentionally Left Blank

# Responding to Defense Demands for Government Assistance in Large ESI Criminal Cases

*John W. M. Claud*

*Trial Attorney*

*Consumer Protection Branch*

*United States Department of Justice*

Voluminous discovery productions affect every stage of the Department of Justice’s criminal cases. Investigations have become more data-driven, and prosecuting even seemingly simple cases often hinges on reliable data management as much as reliable witness testimony. Prosecutors’ obligations dealing with electronically stored information (“ESI”) have also changed, and Department lawyers handle ESI assiduously so that they can understand the full scope of what they have collected, discern the significance of the evidence, and meet stringent discovery obligations.<sup>1</sup>

Part of successfully navigating the criminal ESI landscape includes responding to increasingly common defense demands that prosecutors help them somehow manage and organize ESI turned over in discovery. Sometimes these entreaties are understandable requests from defense lawyers who are restricted by financial limitations or truly overwhelmed with the technical aspects of dealing with large amounts of data. However, defense attorneys may use less principled demands for additional government resources to delay cases, gain access to prosecutors’ trial strategies, or assert a meritless *Brady* violation.<sup>2</sup>

These kinds of requests can put prosecutors between a Scylla of unwillingly helping defendants prepare their defense cases for them and a Charybdis of keeping cases on track towards a trial date. The immediate retort to such a request of “do your own job” may be well-supported in case law,<sup>3</sup> but in a case

---

<sup>1</sup> The Department’s discovery guidelines are broad in scope and crucial to the function of justice. These responsibilities are laid out in numerous resources that include: FED. R. CRIM. P. 16; the Jencks Act, (18 U.S.C.A. §3500 (West)); the U.S. Attorney’s Manual at §9-5.001; the Department’s 2010 Guidance for Prosecutors Regarding Criminal Discovery (the “Ogden Memo”); the Department’s 2011 Guidance on the Use, Preservation, and Disclosure of Electronic Communications in Federal Criminal Cases; the 2012 Joint Electronic Technology Working Group (“JETWG”) Recommendations for Electronically Stored Information (ESI) Discovery Production in Federal Criminal Cases; the Department’s March 2014 Guidance on the Personal Use of Social Media by Department Employees; the Department’s May 2014 Amendment of Section 9-5.100 of the U.S. Attorneys’ Manual (the “Giglio Policy”); the 2016 JETWG Guidance on ESI Discovery to Detainees; and, the 2017 Supplemental Guidance for Prosecutors Regarding Criminal Discovery Involving Forensic Evidence and Experts.

<sup>2</sup> *Brady v. Maryland*, 373 U.S. 83 (1963).

<sup>3</sup> *See, e.g., Polzin v. Mutter*, 503 F. App’x 474, 476 (7th Cir. 2013) (“The Due Process Clause, whether generally or as interpreted in *Brady*, does not impose a constitutional duty on the state to search for, or assist a defendant in developing, mitigating evidence.”); *Werth v. United States*, 493 F. App’x 361, 366 (4th Cir. 2012) (“The defendants seem to contend that under *Brady* and its progeny, the government was somehow obligated to conduct its own investigation of the incidents and turn over the results of that investigation to the defense. This argument is without merit.”); *United States v. Gray*, 648 F.3d 562, 567 (7th Cir. 2011) (The government “had no duty to . . . conduct the defense’s investigation for it.”); *Odem v. Hopkins*, 192 F.3d 772, 777 (8th Cir. 1999) (“*Brady* imposes no obligation on the State to reveal the exculpatory nature of the evidence being turned over but only requires complete disclosure to the defense . . . To rule otherwise would impose a duty on the prosecution to do the defense’s work, and broaden

involving large amounts of data, it may not appease judges who want to move cases to trial, are sympathetic to the plight of a seemingly-overwhelmed defense attorney, or look to keep a record that will survive post-trial review.

So what are a prosecutor's options when a defendant either asks for help with complex data discovery from the prosecution, or goes to the court and demands it?

## I. Challenges Prosecutors Face: The Kinds of Requests Defendants May Make

In broadest terms, recent court battles in this area have centered around two general types of demands on prosecutors. The first are demands relating to locating specific, ostensibly exculpatory evidence within a larger set of data. The second are often more nettlesome demands to do something more with produced electronic discovery—reprocessing, reworking, or reorganizing data in some way to make access easier for the defense's pretrial convenience.

### A. The First Step: Producing Electronic Discovery in a Searchable, Usable Form

Simple organizational measures can help deflect either of these kinds of requests as trial approaches. Defeating defendants' excessive e-discovery demands often rests on how usable and accessible prosecutors make their discovery productions when they turn them over. The most important measure prosecutors can take to forestall an unreasonable court order is to put thought and effort into making discovery productions organized and searchable.<sup>4</sup>

The JETWG's 2012 protocol contains several key principles implicated in ESI discovery that, when followed, put prosecutors in a much better position to defend against defense requests to do more with discovery data. Principle Three of the protocol commands that at "the outset of a case, the parties should meet and confer about the nature, volume, and mechanics of producing ESI discovery . . . an on-going dialogue may be helpful."<sup>5</sup> Principle Four commands that "parties should discuss what formats of production are possible and appropriate, and what formats can be generated. Any format selected for producing discovery should maintain the ESI's integrity, allow for reasonable usability, reasonably limit costs, and, if possible, conform to industry standards for the format."<sup>6</sup> Principle Five commands that "[w]hen producing ESI discovery, a party should not be required to take on substantial additional processing or format conversion costs and burdens beyond what the party has already done or would do for its own case preparation or discovery production."<sup>7</sup> Finally, Principle Nine commands that the "parties should make good faith efforts to discuss and resolve disputes over ESI discovery, involving those with the requisite technical knowledge when necessary, and they should consult with a supervisor, or obtain

---

*Brady* beyond its dictate of disclosure to include a requirement as to the manner of the disclosure."); *United States v. Mmahat*, 106 F.3d 89, 94 (5th Cir. 1997) ("[T]here is no authority for the proposition that the government's *Brady* obligations require it to point the defense to specific documents within a larger mass of material that it has already turned over."); *United States v. Hill*, 2016 WL 8674241, at 10 (E.D. Mo. Aug. 5, 2016) ("The government does not have a duty to do [a defendant's] work for her.").

<sup>4</sup> When prosecutors fail to make reasonable efforts to assist defense counsel, judges sometimes impose onerous requirements on prosecutors to level the playing field. *See, e.g.*, *United States v. Sherifi*, 2012 WL 3260251 (E.D.N.C. Aug. 8, 2012) (judicial order requiring prosecutors to transcribe numerous audio recordings even though the government did not intend to use those recordings as evidence.).

<sup>5</sup> *See* Recommendations for Electronically Stored Information (ESI) Discovery Production in Federal Criminal Cases (Feb. 2012) at 2.

<sup>6</sup> *Id.* at 2-3.

<sup>7</sup> *Id.* at 3.

supervisory authorization, before seeking judicial resolution” of any disputes.<sup>8</sup> Prosecutors that follow the Protocol’s guidance anticipate and avoid many of the potential roadblocks defendants may try to construct as cases move towards trial.

Aside from Departmental guidance, the case law is also overwhelmingly clear on this issue: the government’s obligation is to produce discovery information transparently, in a manner that the defense can use and access. However, aside from that wide-ranging requirement, our *Brady* obligations, in and of themselves, do not place additional burdens on the specific manner that ESI is provided to defendants.<sup>9</sup> In *United States v. Warshak*, the Sixth Circuit pointed out that Rule 16 “is entirely silent on the issue of the form that discovery must take; it contains no indication that documents must be organized or indexed.”<sup>10</sup> That leaves the organization to the prosecution; the government is in the best position to determine the specific form discovery takes as long as it is usable and accessible.<sup>11</sup> In other words, when defendants demand more from the government, the overarching consideration judges should consider is whether the discovery information is accessible to the defense, not whether it is in a form the defense prefers.

So what constitutes producing ESI in usable, accessible form? Rulings since *Warshak* at both the District and Circuit Court level have provided helpful guidance for prosecutors to organize e-discovery productions and deflect unprincipled defense requests. Specific case rulings guide prosecutors to:

- identify the sources of seized items;<sup>12</sup>
- provide materials in a “load-ready” file format that can be easily searched;<sup>13</sup>
- provide searchable copies of documents,<sup>14</sup> or provide discovery in an electronically searchable database;<sup>15</sup>
- thoroughly index audio and make it as searchable as possible;<sup>16</sup>
- meet with defense counsel and recommend where they focus their review efforts;<sup>17</sup>
- provide indices to the defendants, and direct defendants to where they can find the most relevant information;<sup>18</sup>
- present evidence pretrial in an attempt to persuade defendants to cooperate;<sup>19</sup>
- identify “hot docs” the government is likely to use as trial exhibits;<sup>20</sup>
- provide any trial exhibits used in any case against codefendants;<sup>21</sup>

---

<sup>8</sup> *Id.*

<sup>9</sup> See *United States v. Dunning*, 2009 WL 3815739, at 1 (D. Ariz. Nov. 12, 2009) (“*Brady* does not mean that the Government must take the evidence that it has already disclosed to Defendant, sift through this evidence, and organize it for Defendant’s convenience.”).

<sup>10</sup> *United States v. Warshak*, 631 F.3d 266, 296 (6th Cir. 2010).

<sup>11</sup> *United States v. Briggs*, 2011 WL 4017886, at 8 (W.D.N.Y. Sept. 8, 2011).

<sup>12</sup> *United States v. Vujanic*, 2014 WL 3868448, at 2 (N.D. Tex. Aug. 6, 2014).

<sup>13</sup> *United States v. Weaver*, 992 F. Supp. 2d 152, 156 (E.D.N.Y. 2014).

<sup>14</sup> *United States v. Skilling*, 554 F.3d 529, 577 (5th Cir. 2009).

<sup>15</sup> *United States v. Ohle*, 2011 WL 651849, at 4 (S.D.N.Y. Feb. 7, 2011).

<sup>16</sup> *United States v. Rubin Chambers*, 825 F.Supp. 451, 457 (S.D.N.Y. 2011). See also *Sherifi*, 2012 WL 3260251 at 3.

<sup>17</sup> *United States v. Simpson*, 2011 WL 978235 at 8 (N.D. Tex. Mar. 21, 2011).

<sup>18</sup> *United States v. Parnell*, 32 F. Supp. 3d 1300, 1309 (M.D. Ga. 2014).

<sup>19</sup> *Ohle*, 2011 WL 651849 at 2.

<sup>20</sup> *United States v. Godfrey*, 2013 WL 1414887, at 2 (D. Mass. Apr. 5, 2013).

<sup>21</sup> *Vujanic*, 2014 WL 3868448, at 2.

- through the court, ensure that the defendant is provided with appropriate software to comb through the evidence and employ the services of a computer technician;<sup>22</sup>
- encourage the appointment of a coordinating discovery attorney;<sup>23</sup>
- offer to clarify points of confusion for defense counsel;<sup>24</sup>
- note the size of the defense team, which may be relevant to defeat a later claim of inadequate resources;<sup>25</sup> and,
- generally work to facilitate the defense’s review of the files both before and during the trial.<sup>26</sup>

The rulings from these cases all speak to the same general theme: if prosecutors take time to appropriately organize productions and put defendants in a place where they are “just as likely to uncover the purportedly exculpatory evidence as was the Government,” then further requests for particular formats or functionality likely will not be successful.<sup>27</sup>

## **B. Responding to Demands to Locate Specific Evidence Within a Large ESI Discovery Production**

Once material is made accessible, how far do prosecutors need to go to identify *Brady* in otherwise usable, accessible ESI productions? If ESI discovery is in a usable form, the case law informs us that prosecutors are not also charged with affirmatively searching massive amounts of data to single out every last piece of potentially exculpatory evidence. Courts have consistently ruled that defendants are in a better position than prosecutors to find and determine what is and is not *Brady*.

In *United States v. Skilling*, the defendant claimed that the prosecutors were required to identify potential *Brady* information in voluminous discovery.<sup>28</sup> The Fifth Circuit determined that the prosecutors were not required to do so because the government “did much more than drop several hundred million pages on Skilling’s doorstep.”<sup>29</sup> Government attorneys indexed the electronic files, made them searchable, and highlighted particularly relevant documents.<sup>30</sup> The *Skilling* court noted the potential dangers of prosecutors conducting a *Brady* search when it wrote that the government “was in no better position to locate any potentially exculpatory evidence than was Skilling.”<sup>31</sup> The problem is that *Brady* is in the eye of the beholder: a prosecutor may view what a defense attorney thinks is exculpatory data as valuable, incriminating evidence.<sup>32</sup> *Skilling* and its progeny, which are specifically co-opted in the Ogden memo, provide guidance to avoid this potential problem altogether.<sup>33</sup>

<sup>22</sup> *United States v. Parnell*, 2015 WL 5559818, at 2 (M.D. Ga. Sept. 18, 2015).

<sup>23</sup> *Vujanic*, 2014 WL 3868448, at 2.

<sup>24</sup> *United States v. Henderson*, 2016 WL 7377118, at 2 (E.D. Va. Dec. 20, 2016).

<sup>25</sup> *Rubin Chambers*, 825 F.Supp. 451, 456 (S.D.N.Y. 2011).

<sup>26</sup> *United States v. Richards*, 659 F.3d 527, 545 (6th Cir. 2011).

<sup>27</sup> *Ohle*, 2011 WL651849 at 4.

<sup>28</sup> *Skilling*, 554 F.3d at 576-77.

<sup>29</sup> *Id.* at 577.

<sup>30</sup> *Id.*

<sup>31</sup> *Id.*

<sup>32</sup> *See, e.g., United States v. Cadden*, 2015 WL 5737144, at 3 (D. Mass. Sept. 30, 2015) (“. . . one man's *Brady* item is another woman's smoking gun.”).

<sup>33</sup> *See* Guidance for Prosecutors Regarding Criminal Discovery (“Ogden Memo,” January 4, 2010) (“In cases involving voluminous evidence obtained from third parties, prosecutors should consider providing defense access to the voluminous documents to avoid the possibility that a well-intentioned review process nonetheless fails to identify material discoverable evidence.”).

Several other cases have emphasized that there is no authority that commands the prosecution to “root out” potentially exculpatory evidence from a large mass of discovery.<sup>34</sup> These holdings are especially applicable to data that originally comes from a target company. ESI seized from targets through a search warrant, for example, is understandably more immune to defense demands for particularized searching than data from third parties.<sup>35</sup> In reaching its decision in *Warshak*, the court noted that much of the data the defendant wanted additional government resources to sort out was originally his own material, seized in the investigation.<sup>36</sup>

There are, however, some special circumstances that may exist that would drive a court to order the government to affirmatively identify *Brady* in a large trove. Based upon the unusual facts in *United States v. Salyer*, the court ordered the government to scour voluminous materials and identify documents that “may” be *Brady* material.<sup>37</sup> The sole defendant was incarcerated, had a small defense team, lacked the benefit of any parallel civil investigation, and could not access any computers to view discovery. However, the judge in *Salyer* also carefully limited his decision, writing that it was not generally applicable to other cases. In fact, discovery review problems facing an incarcerated defendant<sup>38</sup> with limited access to software tools can be remedied in other ways, as in *United States v. Graves*.<sup>39</sup> There, the court simply granted an incarcerated defendant a continuance, appointed a pretrial investigator to help the defendant review ESI discovery, and ordered the Marshal Service to grant him “adequate computer access” either at his detention facility or at the courthouse.<sup>40</sup>

As Department guidance enumerates, the large size of discovery does not shield prosecutors from identifying and turning over data encountered in the course of their investigation that they affirmatively determine is exculpatory.<sup>41</sup> The *Skilling* court made the same point when it wrote that “it should go without saying that the government may not hide *Brady* material of which it is actually aware in a huge open file in the hope that the defendant will never find it.”<sup>42</sup> This idea was reiterated in *United States v. Blankenship*, where the court ruled that the government should identify *Brady* material it had affirmatively collected and set aside.<sup>43</sup>

The *Blankenship* court did not require prosecutors to scour their database in a search for as-yet-unidentified exculpatory evidence. Yet, absent the duty to scour, prosecutors should still be mindful not to obscure incriminating ESI as a litigation strategy, even when doing so is not specifically a *Brady* violation. In *United States v. Stirling*, the prosecution discovered recordings of highly incriminating Skype chats during its investigation.<sup>44</sup> The government turned the chats over in discovery,

---

<sup>34</sup> *Warshak*, 631 F.3d at 297; *United States v. AU Optronics Corp.*, 2011 WL 6778520, at 1 (N.D. Cal. Dec. 23, 2011); *United States v. Alvarado*, 2001 WL 1631396, at 4 (S.D.N.Y. Dec. 19, 2001).

<sup>35</sup> *Id.* See also, e.g., *United States v. George*, 684 F. App'x 223, 226 (3d Cir. 2017) (rejecting defendant's assertion that an unreadable production containing information from his own bank accounts constituted a *Brady* violation.); *United States v. Meredith*, 2015 WL 5570033, at 3 (W.D. Ky. Sept. 22, 2015) (rejecting defendant's motion to compel *Brady* production in part because “the particular hard drives referenced in Defendant's complaint were those drives taken from his laptop and desktop.”).

<sup>36</sup> *Warshak*, 631 F.3d at 297.

<sup>37</sup> *United States v. Salyer*, 2010 WL 3036444 at 3 (E.D. Cal. Aug. 2, 2010).

<sup>38</sup> Prosecutors who are handling cases with incarcerated defendants are well-advised to consult the Department's Guidance for the Provision of ESI to Detainees, produced by the JETWG in 2016.

<sup>39</sup> *United States v. Graves*, 856 F.3d 567, 570 (8th Cir. 2017).

<sup>40</sup> *Id.* at 569.

<sup>41</sup> See Ogden Memo (“[T]he format of the information does not determine whether it is discoverable. For example, material exculpatory information that the prosecutor receives during a conversation with an agent or a witness is no less discoverable than if that same information were contained in an email.”).

<sup>42</sup> *Skilling*, 554 F.3d at 577.

<sup>43</sup> *United States v. Blankenship*, 2015 WL 3687864, at 7 (S.D.W. Va. June 12, 2015).

<sup>44</sup> *Stirling*, 2012 WL 12926045 at 1.

but they were not readily apparent in the production; a specific program was necessary to locate them on a seized hard drive. Despite warnings to the defense that the defendant should not testify, the prosecutors did not produce the specific chats until their rebuttal case, after the defendant had taken the stand in his own defense.<sup>45</sup> The chats completely eviscerated the defendant's testimony, resulting in a conviction. The district judge, however, granted a new trial, reasoning that while the prosecution had satisfied its basic discovery obligations, its failure to identify that specific evidence or the means to find it demanded a new trial in the interests of justice.<sup>46</sup> The takeaway from *Stirling* is that data is not meaningfully produced if additional steps, like special software, are required to review it. Like *Salyer*, *Stirling* is limited in its holding, and no other cases have cited it as authority, but it counsels prosecutors to favor ESI usability and transparency over trial strategy.

### C. Responding to Demands for Additional Data Management or Support

Other than demanding that prosecutors locate specific data within a production, the complex nature of electronic data may provide defense attorneys a number of other opportunities to accuse the government of misfeasance. In some recent cases, defense attorneys have asserted that the government has somehow technically mishandled ESI, asked the government to cull material from a production, demanded paper files that stand apart from ESI, and pleaded for additional data manipulation in support of their defense theories. These claims all highlight the need for care and diligence when managing large sets of ESI through all phases of investigations and subsequent discovery productions.

For example, when prosecutors first receive large troves of data, either through the execution of a search warrant, from a grand jury subpoena, or other sources, they ought to devise and employ methods to identify and extract relevant material from the heaps of extraneous data that will inevitably accompany the production. That is usually accomplished through a combination of employing date restrictions, custodian identifications, and keyword searches. Culling irrelevant data from your mass of evidence is crucial so that prosecutors can avoid spending time reading useless personal email or spam rather than communications between targets. After this process, however it is employed, two buckets of data will remain: (1) relevant data that the prosecution team will need to process further, then search, review, and investigate; and, (2) irrelevant data that is not processed, but that the prosecution ought to maintain in its pristine form.

However, what prosecutors may view as unprocessed and extraneous may become a target for defense attorneys approaching trial. Citing the government's obligation under *Brady*, defendants may request that the Department process and produce irrelevant data, arguing that it, too, must be searched for exculpatory material. In actuality, defendants may not actually want it, but pointing to a mass of unviewed data may be a tempting target for defendants trying to delay a case.

In order to defeat potential *Brady* claims, prosecutors have two options when dealing with data they deem irrelevant. First, they can give a copy of their unprocessed data to the defense. In *United States v. Parnell* and its attendant cases, the Department attorneys gave defense teams copies of all of the unprocessed forensic images, separated from the load-ready processed data. At that point, the decision about what to do with irrelevant data rested solely with the defense team and the government had satisfied its *Brady* obligation.<sup>47</sup> Another option is to simply offer the defendant the opportunity to inspect and copy the unprocessed, irrelevant data early in the discovery process. Defeating a *Brady* claim may be as simple as adding one sentence to the initial discovery transmittal letter offering the irrelevant ESI to the

---

<sup>45</sup> *Id.*

<sup>46</sup> *Id.* at 2.

<sup>47</sup> See *United States v. Parnell*, 2015 WL 5559818, at 2 (M.D. Ga. Sept. 18, 2015) (Defendant received all data from government, was granted multiple continuances, was provided software to search the data, and employed a computer technician to help her.).

defendants, in unprocessed form, at the outset of discovery. At that point, the responsibility again falls to defendants to make a decision about it.

In *United States v. Cadden*, the defendant claimed that the methods the government used to cull irrelevant data may have left exculpatory material out of the discovery production.<sup>48</sup> Defense counsel demanded that the government process that irrelevant data and search it, that the court delay the trial date, and that the court assign a Federal agent to assist the defense in executing its own searches, claiming that the newly processed irrelevant data would have resulted in an increase of ESI to search. The AUSAs defeated this through two methods. First, they employed redundancy when they identified the relevant material, relying on a combination of keyword searching, custodian identities, and appropriate date restrictions to find the data that was truly germane to their investigation. They asserted that these steps represented a thorough, good faith methodology to ensure the culled data was indeed irrelevant. Then, in their first discovery transmittal letter, the prosecutors told the defendants that there was unprocessed, irrelevant data available for inspection and copying. Unsurprisingly, when it was initially offered, none of the defendants involved in the case jumped at the chance to obtain and process gigabytes of data the government deemed to be irrelevant. The defendants in *Cadden* waited until the end of the discovery period to make their motion, nearly a year after the USAO first produced discovery. All of these factors led the court to reject the defense request.

A defendant's request for additional manipulation or reprocessing may also implicate the government's duty not only to include irrelevant files, but also to recover deleted files. In *United States v. Dunning*, the defendant claimed that prosecutors should have forensically recovered information that was deleted from a hard drive seized from a third party,<sup>49</sup> asserting that the failure to do so was a *Brady* violation. However, the government did not delete the files at issue. The entity from whom the government seized the drives deleted the information before the government obtained it. The court ruled that the government had no duty to go back to the third party and recover the data.<sup>50</sup>

Adding information to a production can also have its perils. The axiom that "no good deed goes unpunished" was proven in *United States v. Shabudin*, where prosecutors hosted a database and, in an effort to streamline the discovery process, allowed the defense to have access to it.<sup>51</sup> The prosecutors agreed with the defense on the scope and duration of the database, including funding and staffing for the project for two years at an anticipated cost of nearly \$2 million. In addition to the database, the case involved some paper discovery. Initially, the prosecutors did not upload the paper material to the database, but did provide it to the defense. As the case progressed, the defendants demanded that the government add electronic images of the paper materials into the database, and the government agreed to do so.<sup>52</sup> That addition, however, drew down the budget for maintaining the database, and would have closed it months ahead of the initial schedule. Here, the prosecutors' diligence in making the material available to the defense did not suffice, because the court determined that the prosecution did not effectively inform the defendants that adding the additional material would, in effect, close off the Relativity database early. The court ordered the Department to not only maintain the Relativity database, but to continue to pay for non-technical support and paralegal assistance that the defendants demanded. This was so even though the defense still had access to the whole of the discovery material through a Concordance database they maintained at their own expense.<sup>53</sup> That court order resulted in an additional

---

<sup>48</sup> *Cadden*, 1:14-CR-10363, Doc. 531, February 5, 2016 (D. Mass 2016).

<sup>49</sup> *Dunning*, 2009 WL 3815739 at 1.

<sup>50</sup> *Id.* at 2.

<sup>51</sup> *United States v. Shabudin*, 2014 WL 1379717 at 1 (N.D. Cal. Apr. 8, 2014).

<sup>52</sup> *Id.*

<sup>53</sup> *Id.* at 4.

multi-million dollar expense for the government. The lesson from *Shabudin* is that no matter how expeditious or well-intentioned, sharing discovery platforms with defense counsel is rarely a good idea.

However, compare the production additions in *Shabudin* to an issue relating to additional paper discovery raised in *Ohle*. Aside from their demands that the government affirmatively search for *Brady*, the *Ohle* defendants moved the District court for a new trial after prosecutors discovered they had inadvertently failed to include electronic images of 110 boxes of documents in the discovery produced. However, much of the material was included in other forms within the government's production, and the prosecutors made the entire 110 boxes available for inspection prior to the trial.<sup>54</sup> The court ruled that these redundant measures were sufficient, and that there was no *Brady* violation.<sup>55</sup>

Defendants may also ask prosecutors to remove data that survived initial processing, arguing that it unnecessarily burdens discovery, removing it from its usable, accessible form. In *United States v. Meredith*, the defendant moved the court to compel the government to spend \$300,000 to reprocess an extensive discovery production in order to remove what he deemed was extraneous data such as personal emails.<sup>56</sup> The defendant there claimed that the data was not relevant to the case and obstructed his ability to review what was turned over. The court in *Meredith* rejected the request because the ESI was searchable, and noted that the government had no duty to remove documents from the production. The court also noted that the prosecutors had provided ample oral and written assistance to the defendant in searching for files so that the alleged "extra" ESI was not a hindrance.<sup>57</sup>

Finally, in an effort to create potentially exculpatory evidence, defendants may demand that prosecutors analyze or sort existing data in a certain way to create new, mined information. Just as prosecutors are not required to contribute to a defense investigation, they are not required to perform additional data analysis aside from what they did as part of their own investigation. In *United States v. Gray*,<sup>58</sup> the prosecutors had created their own analysis of payment records in a Medicaid fraud case as they prepared for trial, and they turned that information over, along with the original underlying data. On appeal of his conviction, the defendant asserted that the government should have employed a Medicaid bill processor to run a different forensic computer analysis of the data that would have revealed information about a possible co-conspirator. That analysis, he argued, may have potentially helped the defense at trial demonstrate a lesser role for Gray in the fraud. The Seventh Circuit rejected that argument, finding that having turned over the underlying data as well its own analyses, the prosecutors "had no duty to go further and conduct the defense's investigation for it."<sup>59</sup>

Other courts have taken a similarly restrictive view of ordering the government to provide active litigation support when the underlying factual information central to the defense's request was produced in discovery. This includes allowing defense access to government computers. For example, in *United States v. Schmidt*, the court denied a defendant's request to access summary material on IRS computers when the defense had longstanding access to underlying reports that were produced in discovery.<sup>60</sup>

## II. Practice Tips Distilled from the Case Law

Prosecutors' responses to motions demanding these kinds of ESI discovery assistance have included some common recitals of information that put judges and magistrates in a good position to

---

<sup>54</sup> See *Ohle*, 2011 WL 651849 at 2.

<sup>55</sup> *Id.* at 4.

<sup>56</sup> *Meredith*, 2015 WL 5570033 at 1.

<sup>57</sup> *Id.* at 2.

<sup>58</sup> *Gray*, 648 F.3d 562.

<sup>59</sup> *Id.* at 567.

<sup>60</sup> *United States v. Schmidt*, 2007 WL 1232180, at 1 (D. Colo. Apr. 25, 2007).

understand the particular issue and make favorable rulings. Any response to such a motion is well-served to include the following:

- an outline of all the steps the prosecution team took to provide discovery, with specific accounting of pages or documents produced;
- an outline of how the prosecution team handled the processing of ESI to ensure it could be produced in a usable form to defense counsel;
- an outline of how irrelevant data was culled, either through searches for all custodians of note, names, key words, date restrictions, or any technology assisted review that was employed;
- a description of any offers to make that irrelevant material available for inspection or production, which should be included in the first transmittal letter relating to ESI production;
- a recitation of specific efforts made to make discovery accessible, organized, and searchable;
- specific descriptions of the databases used to make searching easier, including those databases' searchability parameters;
- an outline of the resources available to the defense, including a description of the size of the defense team, its technical capabilities, and the presence of a coordinating discovery attorney;
- a recitation of discussions with defense attorneys about how the discovery is produced, and any assistance offered or given; and,
- a description of the defendant's own knowledge and ability to assist his or her own defense team in searching for and managing the discovery material.

Of course, prosecutors cannot make these responsive legal arguments unless they keep their own files organized and the evidence searchable as their investigation progresses. Good organization helps prosecutors create reasonable discovery productions. Thus, preparing for discovery while still in the investigative phase of a case puts Department lawyers in a position to meet their discovery obligations, successfully deflect defense demands to go beyond their duties, and affect justice.

#### **ABOUT THE AUTHOR**

**John W. M. Claud** has been a Trial Attorney in the Consumer Protection Branch of the Civil Division since 2008. He prosecutes criminal matters that involve the Food, Drug, and Cosmetic Act, as well as complex nationwide fraud schemes that affect consumers across the country.

Page Intentionally Left Blank

# The Resurgence of Denaturalization: The Supreme Court’s Decision in *Maslenjak* and Its Initial Impact on Civil and Criminal Cases Seeking Revocation of U.S. Citizenship

*Timothy M. Belsan*

*Deputy Chief*

*National Security and Affirmative Litigation Unit*

*District Court Section*

*Office of Immigration Litigation*

*Civil Division*

*Aram A. Gavoor*

*Senior Counsel for National Security*

*National Security and Affirmative Litigation Unit*

*District Court Section*

*Office of Immigration Litigation*

*Civil Division*

*Joseph A. Marutollo*

*Chief, Immigration Litigation*

*United States Attorney’s Office*

*Eastern District of New York*

## I. Introduction<sup>1</sup>

For the first time in nearly three decades, the Supreme Court has waded back into the waters of denaturalization. Last term, the Court decided *Maslenjak v. United States*,<sup>2</sup> a case involving the conviction and denaturalization of an individual who knowingly lied during the refugee and naturalization processes regarding her husband’s military service during the Bosnia War. The Court’s decision limited the scope of the criminal statute that carries with it as a penalty the revocation of United States citizenship, 18 U.S.C. § 1425(a), and provided an interpretation of the statute’s structure of which prosecutors should be aware. Although *Maslenjak* also discussed the civil denaturalization statute, 8 U.S.C. § 1451, the Supreme Court specifically limited its decision to a subcategory of cases brought under 18 U.S.C. § 1425(a). This article will provide a brief background on *Maslenjak*, and then discuss the Supreme Court’s decision and the impact it is beginning to have on denaturalization cases around the

---

<sup>1</sup> The authors wish to thank the Criminal Division’s Human Rights and Special Prosecutions Section for its assistance during the preparation of this article.

<sup>2</sup> *Maslenjak v. United States*, 137 S. Ct. 1918 (2017).

Country, both on criminal prosecutions under 18 U.S.C. § 1425 and on civil cases brought under 8 U.S.C. § 1451.

## II. Background of *Maslenjak*<sup>3</sup>

In the 1990s, Divna Maslenjak, an ethnic Serb, resided in what is today Bosnia and Herzegovina, while the civil war between Serbs and Muslims divided the new country. In April 1998, she and her family met with an American immigration official in Belgrade to seek refugee status in the United States. Interviewed under oath, Maslenjak—who was the primary applicant for her family’s refugee application—explained that the family feared persecution in Bosnia from both sides of the conflict. Of particular note, Maslenjak stated under oath that her family feared persecution from the Serbs because her husband had evaded service in the Bosnian Serb Army by absconding to Serbia, where he remained separated from the family for nearly five years to avoid conscription. Based on those representations, Maslenjak and her family, including her husband, were granted refugee status and immigrated to the United States in 2000.

Six years later, Maslenjak applied for naturalization. Question 23 on the naturalization application form asked whether she had ever given “false or misleading information” to a government official while applying for an immigration benefit. Question 24 similarly asked whether she had ever “lied to a [ ] government official to gain entry or admission into the United States.” Maslenjak answered “no” to both questions, signing her application under penalty of perjury. She also swore that all her written answers were true during a subsequent naturalization interview with a U.S. Citizenship and Immigration Services official. Based on the information in her naturalization application and her testimony during her naturalization interview, Maslenjak was naturalized as a United States citizen in August 2007.

Maslenjak’s representations on her naturalization application, however, were indisputably knowingly false. Only weeks before she filed her naturalization application, Maslenjak was present when immigration officers interviewed her husband about his prior military service, confronting him with military records establishing he had been an officer in the Bosnian Serb Army and had served in a brigade that participated in the infamous Srebrenica massacre. And only a week before she applied for naturalization, her husband was arrested for making a false statement in a government document. During the subsequent criminal proceedings against her husband, Maslenjak admitted she had known all along that her husband spent the war years not evading conscription in Serbia but fighting in Bosnia. Following her husband’s conviction, which rendered him subject to removal from the United States, Maslenjak filed an immigration petition seeking to classify him as the spouse of a United States citizen and allow him to seek permanent resident status as relief from removal.

In light of Maslenjak’s misrepresentations and false testimony, which became apparent during her husband’s criminal proceedings, the government charged her with knowingly “procur[ing], contrary to law, [her] naturalization,” in violation of 18 U.S.C. § 1425(a),<sup>4</sup> which makes it a crime to “knowingly procure[] or attempt[] to procure, contrary to law, the naturalization of any person.”<sup>5</sup> The government argued that Maslenjak violated § 1425(a)<sup>6</sup> because, in the course of procuring her naturalization, she violated another statute: 18 U.S.C. § 1015(a),<sup>7</sup> which prohibits knowingly making a false statement under oath in a naturalization proceeding. Specifically, the government pointed to Maslenjak’s answers to

---

<sup>3</sup> The facts are taken from the Supreme Court’s opinion and the government’s Supreme Court brief. *See* Maslenjak, 137 S. Ct at 1923-24; *see also* Brief for the United States at 2-3, *Maslenjak v. United States*, 137 S. Ct. 1918 (2017) (No. 16-309), 2017 WL 1175619, at 1-4.

<sup>4</sup> 18 U.S.C. § 1425(a) (2012).

<sup>5</sup> *Id.*

<sup>6</sup> *Id.*

<sup>7</sup> 18 U.S.C. § 1015(a) (2012).

questions 23 and 24 on the naturalization application and her corresponding testimony during the naturalization interview. Notably, the District Court instructed the jury that a conviction was proper so long as “the [g]overnment ‘prove[d] that one of the defendant’s statements was false’—even if the statement was not ‘material’ and ‘did not influence the decision to approve [her] naturalization.’”<sup>8</sup> The jury returned a guilty verdict, and the United States Court of Appeals for the Sixth Circuit affirmed the conviction on appeal. In particular, the Sixth Circuit upheld the District Court’s instruction that Maslenjak’s false statements need not have influenced U.S. Citizenship and Immigration Services (USCIS) decision on whether to grant her naturalization application.

### III. The Supreme Court’s Holding in *Maslenjak*

The Supreme Court granted certiorari in *Maslenjak* to resolve a circuit split<sup>9</sup> on the issue of whether making a false statement during naturalization proceedings in violation of 18 U.S.C. § 1015(a) results in a violation of 18 U.S.C. § 1425(a) irrespective of whether the false statement was material to obtaining citizenship.<sup>10</sup> Chief Justice John Roberts presented a hypothetical at oral argument that highlighted the distinction: whether a statement by a naturalization applicant that he had never committed a crime or offense, when he knew many years prior he had driven in excess of the speed limit, would permit the government to, “20 years after [he] was naturalized as a citizen . . . knock on [his] door and say, guess what, you’re not an American citizen after all” despite the fact that the speeding violation would not have rendered him ineligible at the time he naturalized.<sup>11</sup> When the Assistant to the Solicitor General provided an affirmative response, other justices joined with questions about the apparently broad nature of the questions listed on the naturalization form, and their concern about the materiality of every such omission on the form.<sup>12</sup>

In the end, the Supreme Court’s majority opinion did not address the materiality issue. Rather, the Court found that the text of § 1425(a) (“procure[ ], contrary to law, . . . naturalization”) requires that “the illegal act must have somehow contributed to the obtaining of citizenship,” and remanded Maslenjak’s case for further proceedings.<sup>13</sup> *Maslenjak* held that in order to obtain a conviction under 18 U.S.C. § 1425(a) “the [g]overnment must establish that an illegal act by the defendant played some role in her acquisition of citizenship,” or what the Court elsewhere referred to as a “causal relation.”<sup>14</sup> More specifically, the Court held that “[w]hen the illegal act is a false statement,” the government must demonstrate “that the defendant lied about facts that would have mattered to an immigration official, because they would have justified denying naturalization or would predictably have led to other facts warranting that result.”<sup>15</sup>

The Court noted that the government could prove such causal relation in one of two ways. Most simply, the government can put forward evidence that “the facts the defendant misrepresented are themselves disqualifying” for naturalization.<sup>16</sup> For example, an applicant might lie about the extent of his

---

<sup>8</sup> *Maslenjak*, 137 S. Ct. at 1924.

<sup>9</sup> Compare *United States v. Maslenjak*, 821 F.3d 675, 685-86 (6th Cir. 2016) (false statements need not have influenced the naturalization decision), with *United States v. Munyenyezi*, 781 F.3d 532, 536 (1st Cir. 2015) (requiring the government to make some showing that a misrepresentation mattered to the naturalization decision); *United States v. Latchin*, 554 F.3d 709, 712-15 (7th Cir. 2009) (same); *United States v. Alferahin*, 433 F.3d 1148, 1154-56 (9th Cir. 2006) (same); *United States v. Aladekoba*, 61 F. App’x. 27, 28 (4th Cir. 2003) (same).

<sup>10</sup> *Maslenjak*, 137 S. Ct. at 1924.

<sup>11</sup> *Maslenjak v. United States*, 2017 WL 1495528 (U.S.), 27-28 (U.S. Oral. Arg., 2017).

<sup>12</sup> *Id.*

<sup>13</sup> *Maslenjak*, 137 S. Ct. at 1921-23, 1931.

<sup>14</sup> *Id.* at 1923.

<sup>15</sup> *Id.*

<sup>16</sup> *Id.* at 1928.

travel to suggest that he met the physical presence requirement for naturalization when in fact he did not.<sup>17</sup>

Even where the government cannot show the deception concealed clear ineligibility for citizenship, however, the Court noted that an applicant’s lie might still have “the requisite bearing on a naturalization decision.”<sup>18</sup> To satisfy this second, alternative method of proving causal relation (which the Court labeled the “investigation-based theory”), the government “can rest on disqualifications that a thwarted investigation predictably would have uncovered.”<sup>19</sup> This requires a two-part showing. First, the government must establish that “the misrepresented fact was sufficiently relevant to a naturalization criterion that it would have prompted reasonable officials, ‘seeking only evidence concerning citizenship qualifications,’ to undertake further investigation.”<sup>20</sup> Second, the government must show that the further investigation, had it occurred, “‘would predictably have disclosed’ some legal disqualification.”<sup>21</sup> The government need not show that the foiled investigation would have absolutely unearthed a disqualifying fact.<sup>22</sup>

Finally, the Court reiterated that a defendant who can affirmatively establish “qualification for citizenship” has an absolute defense because § 1425 “is not a tool for denaturalizing people who . . . were actually qualified for the citizenship they obtained.”<sup>23</sup>

Notably, although the government had argued *inter alia* that Maslenjak’s false statements during the naturalization process were in fact material because they related to whether she and her family had properly been admitted as refugees,<sup>24</sup> the district court instructed the jury that it “could convict based on any false statement in the naturalization process (i.e., any violation of § 1015(a)), no matter how inconsequential to the ultimate decision.” The Supreme Court found the instructions to have been in error and remanded for further proceedings.<sup>25</sup>

Importantly, the Court also highlighted its understanding that “Congress defined two separate crimes in § 1425.”<sup>26</sup> First, as explained in and exemplified by *Maslenjak* itself, § 1425(a) criminalizes illegal means of procurement—i.e., engaging in criminal conduct during the naturalization process that has a causal relation to procuring naturalization.<sup>27</sup> Second, § 1425(b) criminalizes—in the words of the Supreme Court—“simple lack of qualifications” with the appropriate mens rea, analogous to the “illegal procurement” provision in the civil denaturalization statute.<sup>28</sup>

Finally, the Supreme Court confined the impact of *Maslenjak* to criminal false statement cases brought under § 1425(a):

How should § 1425(a)’s requirement of causal influence apply in practice, when charges are brought under that law? Because the proper analysis may vary with the nature of the

---

<sup>17</sup> *Id.*

<sup>18</sup> *Id.* at 1929.

<sup>19</sup> *Id.*

<sup>20</sup> *Id.*

<sup>21</sup> *Id.*

<sup>22</sup> *Id.*

<sup>23</sup> *Id.* at 1930.

<sup>24</sup> See Brief for United States at 48-50, *Maslenjak v. United States*, 137 S. Ct. 1918 (2017) (No 16-309), 2017 WL 1175619.

<sup>25</sup> *Maslenjak*, 137 S. Ct. at 1930-31.

<sup>26</sup> *Id.* at 1925 n.2.

<sup>27</sup> *Id.*

<sup>28</sup> *Id.*; see *Fedorenko v. United States*, 449 U.S. 490, 506 (1981) (indicating that failure to comply with any of the congressionally imposed prerequisites to the acquisition of citizenship renders the citizenship “illegally procured”).

predicate crime, we confine our discussion of that issue to the kind of underlying illegality alleged here: a false statement made to government officials.<sup>29</sup>

Accordingly, *Maslenjak* should have little if any impact on civil denaturalization cases. The materiality and causation standards established in *Kungys v. United States*<sup>30</sup> remain applicable to cases brought under 8 U.S.C. § 1451(a).<sup>31</sup>

## IV. Post-*Maslenjak* Jurisprudence

Since the Court's *Maslenjak* decision was released in late June 2017, a handful of courts have wrestled with its impact on both criminal and civil denaturalization.<sup>32</sup> An examination of these cases gives a sense of how courts will interpret the Supreme Court's decision and provides lessons for prosecuting denaturalization cases post-*Maslenjak*.

### A. Criminal Cases: 18 U.S.C. § 1425

In *United States v. Haroon*,<sup>33</sup> the Sixth Circuit upheld a § 1425(a) conviction against an attack based on the jury instruction.<sup>34</sup> The Court noted that although the *Maslenjak* panel decision that was reversed by the Supreme Court had been Sixth Circuit precedent, “by a quirk of timing, the [*Maslenjak*] panel decision came down three months after Haroon's trial and thus did not affect the district court's jury instructions in this case.”<sup>35</sup> The *Haroon* Court noted that because the underlying § 1425(a) prosecution had been based on a violation of 18 U.S.C. § 1546(a) during the naturalization process, the jury instructions included both materiality and causation elements,<sup>36</sup> and therefore complied with the Supreme Court's decision in *Maslenjak*.

In *United States v. Allouche*, the Fifth Circuit reviewed a conviction under § 1425(b), which makes it a crime for any person, whether for himself or another person not entitled thereto, to “knowingly issue[], procure[], or obtain[] or appl[y] for or otherwise attempt[] to procure or obtain naturalization, or citizenship . . . .”<sup>37</sup> The defendant had been granted naturalization under 8 U.S.C. § 1430, which allows for naturalization after three years of lawful permanent resident status based on living in marital union with a U.S. citizen spouse.<sup>38</sup> Allouche had been a lawful permanent resident for more than five years, so he also met the residency requirement under 8 U.S.C. § 1427, the generally applicable naturalization statute, regardless of his marital relationship.<sup>39</sup> Although Allouche applied for citizenship under both

---

<sup>29</sup> *Maslenjak*, 137 S. Ct. at 1927-28.

<sup>30</sup> *Kungys v. United States*, 485 U.S., 759, 777-79 (1988).

<sup>31</sup> 8 U.S.C. § 1451(a).

<sup>32</sup> While this article addresses the impact of *Maslenjak* on criminal and civil cases, *Maslenjak* has also started to affect decisions in immigration removal proceedings. See *Matter of D-R-*, 27 I. & N. Dec. 105, at 5 (B.I.A. Sept. 14, 2017) (addressing *Maslenjak* and declining to adopt or apply the “fair inference” test set forth in Justice Brennan's concurrence in *Kungys*, 485 U.S. at 783 to questions of inadmissibility under 8 U.S.C. § 1182 (a)(6)(C)(i)).

<sup>33</sup> *United States v. Haroon*, 874 F.3d 479 (6th Cir. 2017).

<sup>34</sup> 18 U.S.C. § 1425(a).

<sup>35</sup> *Haroon*, 874 F.3d. at 479.

<sup>36</sup> *Id.* at 482; 18 U.S.C. § 1546(a).

<sup>37</sup> *United States v. Allouche*, 703 F. App'x 241 (5th Cir. 2017). The appeals panel also reviewed and affirmed Allouche's conviction for making a materially false statement on a security clearance form in violation of 18 U.S.C. § 1001. *Id.* at 242.

<sup>38</sup> *Id.* at 243; see also 8 U.S.C. § 1430.

<sup>39</sup> *Id.* at 242, 245. Allouche's work as an interpreter for the United States military in Iraq excused his extended absences from the United States during that five-year period, which otherwise would have rendered him ineligible under the general residency requirement. *Id.* at 245.

§ 1427 and § 1430, he was naturalized only under § 1430, and the indictment based the § 1425(b) charges only on Allouche’s “allegedly false statements about his marital status and membership in a terrorist organization.”<sup>40</sup> He was acquitted of the latter charge.<sup>41</sup> On appeal from his conviction for false statements concerning his marital status in his naturalization application, Allouche did not challenge the evidence that he had lied about his marital relationship and was separated from his wife at the time he applied to naturalize. He instead argued that the evidence was insufficient to show that he was ineligible for citizenship because he qualified under § 1427. The appellate court agreed.<sup>42</sup>

The Fifth Circuit reversed the § 1425(b) conviction, finding insufficient evidence that the truth of Allouche’s marital status would have had a bearing on his eligibility for naturalization because he could have naturalized under the generally applicable naturalization provision.<sup>43</sup> This finding was predicated, in part, on a misinterpretation of a witness’ testimony that “Allouche could have been eligible to naturalize” under § 1427 to mean that he was in fact eligible to naturalize on that basis.<sup>44</sup> Focusing on the Supreme Court’s “cautionary instruction” in *Maslenjak* that § 1425 “is not a tool for denaturalizing people who . . . were actually qualified for the citizenship they obtained,”<sup>45</sup> the *Allouche* Court rejected the government’s argument and evidence that Allouche was ineligible for citizenship under 8 U.S.C. § 1427(a)(3)<sup>46</sup> for lack of good moral character based upon his false testimony concerning his marriage.<sup>47</sup> The court held that the conviction under § 1425(b) was improper because “the indictment did not allege this conduct, nor did it allege lack of good moral character more generally.”<sup>48</sup> Notably, however, the court did not address the government’s argument that the content of the indictment was legally irrelevant to the defense of eligibility, and that Allouche’s lack of good moral character precluded him from benefitting from this defense.

## B. Civil Cases: 8 U.S.C. § 1451

Only one civil denaturalization case appears to have discussed the Supreme Court’s *Maslenjak* opinion in any extended manner. In *United States v. Ahmed*, the District Court for the Southern District of Ohio ruled in favor of the government after a multi-day bench trial.<sup>49</sup> The district court revoked Ahmed’s naturalized citizenship, concluding that Ahmed had procured such citizenship by concealment of a material fact or by willful misrepresentation, specifically by concealing thirteen trips abroad—each lasting, on average, two to four months—during the five years preceding naturalization.<sup>50</sup> Although the trial occurred more than a year prior to the *Maslenjak* decision, a decision in *Ahmed* had not yet issued when the Supreme Court’s decision in *Maslenjak* was issued. The parties submitted briefs to the district court as to the impact of the Supreme Court’s decision on the then-pending matter. The district court applied *Maslenjak* to the determination of materiality, foregoing any discussion of the fact that *Maslenjak* arose in the context of 18 U.S.C. § 1425 and not 8 U.S.C. § 1451.

The *Ahmed* Court suggested that *Maslenjak* expanded the means by which the government could prove materiality in a civil denaturalization case. First, the court recognized the long-standing test for materiality, “whether the misrepresentation or concealment had a natural tendency to produce the

---

<sup>40</sup> *Id.* at 244.

<sup>41</sup> *Id.*

<sup>42</sup> *Id.* at 241, 244.

<sup>43</sup> *Id.* at 242, 247.

<sup>44</sup> *Id.* at 245-47.

<sup>45</sup> *Id.* at 246-47.

<sup>46</sup> 8 U.S.C. § 1427(a)(3) (2012).

<sup>47</sup> Allouche, 703 F. App’x at 245-47.

<sup>48</sup> *Id.* at 247.

<sup>49</sup> *United States v. Ahmed*, No. 2:12-cv-951, Dkt. No. 65, at 1 (S.D. Ohio. Sept. 20, 2017).

<sup>50</sup> *Id.* at 21, 27-28.

conclusion that the applicant was qualified” for naturalization.<sup>51</sup> It noted that this test corresponded with “the first method” identified in *Maslenjak*.<sup>52</sup> Second, the court held that *Maslenjak*’s “investigation-based theory” allowed for a second means of proving materiality.<sup>53</sup> Under this second method, the government would need to make the two-part showing outlined in *Maslenjak*: (1) that the misrepresented fact was sufficiently related to a naturalization criterion that an immigration official would likely have investigated further; and (2) that the follow-on investigation would “predictably have disclosed” some legal disqualification.<sup>54</sup> The court found that the trips were material to Ahmed’s naturalization under both tests. First, the thirteen trips were material under the traditional test for materiality because the aggregate number of days of travel may have rendered Ahmed ineligible for lack of the requisite physical presence, and individual trips may have been longer than six months, breaking the continuous residence requirement.<sup>55</sup> Second, the destinations of the travel—to countries “known for anti-American terrorism”—and purpose and extent of such travel were relevant to the need to discover potential terrorist affiliations and to ensure appropriate connection to the United States.<sup>56</sup>

## V. Suggestions for Prosecutors Post-*Maslenjak*

As Justice Elena Kagan stated in her majority opinion in *Maslenjak*:

[T]he question of what any individual decision maker might have done with accurate information is beside the point: The defendant in a § 1425 case should neither benefit nor suffer from a wayward official’s deviations from legal requirements. Accordingly, the proper causal inquiry under § 1425(a) is framed in objective terms: To decide whether a defendant acquired citizenship by means of a lie, a jury must evaluate how knowledge of the real facts would have affected a reasonable government official properly applying naturalization law.<sup>57</sup>

This indicates that the government is not required to call as a witness the naturalization examiner who processed the defendant’s application. Rather, the best witness can speak authoritatively regarding naturalization standard operating procedures and eligibility standards at the time of the naturalization application.

In the context of a criminal prosecution under 8 U.S.C. § 1425(a) based on a false statement, prosecutors must invest adequate time to understand the nature of the misrepresentation and how it fits into the agency’s decision whether to grant or deny a naturalization application or to request additional evidence so the agency can properly make such a determination.<sup>58</sup> That understanding will inform how you explain to the jury and the judge the causal link between the false statement(s) and the acquisition of citizenship. The Civil Division’s Office of Immigration Litigation—District Court Section (OIL-DCS), the Criminal Division’s Human Rights and Special Prosecutions Section (HRSP), and the immigration agencies can help with this analysis, as it is a regular part of their day-to-day practice. With a fulsome understanding of the naturalization process and the purpose of the questions on the naturalization application, a false statement can very frequently be shown to have been material to procuring naturalization.

---

<sup>51</sup> *Id.* at 18 (quoting *Kungys*, 485 U.S. at 771).

<sup>52</sup> *Id.*

<sup>53</sup> *Id.* at 19 (citing *Maslenjak*, 137 S. Ct. at 1922).

<sup>54</sup> *Id.*

<sup>55</sup> *Id.* at 22-23.

<sup>56</sup> *Id.* at 23-24.

<sup>57</sup> *Maslenjak*, 137 S. Ct. at 1928.

<sup>58</sup> 8 U.S.C. § 1425(a).

Criminal prosecutors should also consider whether the evidence supports a charge under 18 U.S.C. § 1425(b).<sup>59</sup> In *Maslenjak*, the Supreme Court clarified the scope and differences of the two charges under § 1425, and often there may be evidence that supports charges under both subsections of the statute.<sup>60</sup> In particular, prosecutors should consider whether an individual’s conduct rendered the applicant ineligible for his or her visa or status or prevented him or her from establishing the good moral character required to naturalize,<sup>61</sup> and if so, whether a charge is proper under § 1425(b).<sup>62</sup> For example, false oral testimony under oath during the naturalization interview precludes the individual from establishing good moral character under 8 U.S.C. § 1101(f)(6)<sup>63</sup> so long as the individual gave such testimony for the purpose of obtaining an immigration benefit. A § 1425(b) charge based on ineligibility for false testimony would likely have saved the § 1425(b) count in *Allouche*.<sup>64</sup>

In the civil context, prosecutors have the same options of charging under 8 U.S.C. § 1451(a)<sup>65</sup> based on fraud during the naturalization process (“procured by concealment of a material fact or by willful misrepresentation”) or ineligibility (“illegally procured”).<sup>66</sup> And like the criminal context, the same evidence may support both charges. Regardless of which charge is alleged in a civil case, prosecutors should anticipate that opposing counsel may argue that *Maslenjak* has changed the landscape for civil denaturalization, increasing the burden on the government. Should you find yourself needing to address or brief up the impact of *Maslenjak*, loop in OIL-DCS, who have already been working on briefing and can provide useful language.

Finally, prosecutors should always be mindful of Justice Southerland’s famous advisal, that it is the role of a federal prosecutor to “prosecute with earnestness and vigor,” striking hard blows, but always fair ones.<sup>67</sup> In particular, when it relates to actions seeking to revoke naturalization, prosecutors must continue to be conscious of what is at stake in these cases: namely, as Justice Anthony Kennedy stated during the oral argument in *Maslenjak*, “the priceless value of citizenship.”<sup>68</sup> Thus, not every omission by the defendant in the naturalization process—intentional or not—will mandate denaturalization.

## VI. Conclusion

Ultimately, *Maslenjak* raises the bar for the government to convict naturalized citizens for making false statements in the naturalization application process, as the government must now establish the causal link between false statements and the decision to grant citizenship.

As the above cases demonstrate, post-*Maslenjak* jurisprudence is moving swiftly across the country. If you want to discuss any of the foregoing matters or you have any questions regarding the ways

---

<sup>59</sup> 18 U.S.C. § 1425(b).

<sup>60</sup> *Id.*; *Maslenjak*, 137 S. Ct. at 1925 (providing that “[a]ssuming the appropriate *mens rea*, subsection (a) covers illegal means of procurement, as described above, while subsection (b) covers simple lack of qualifications”).

<sup>61</sup> See 8 U.S.C. § 1421(a)(3). Good moral character is defined in 8 U.S.C. § 1101(f) and 8 C.F.R. § 316.10.

<sup>62</sup> 18 U.S.C. § 1425(b); see *Maslenjak*, 137 S. Ct. at 1926-27 (noting that “[t]he immigration statute requires all applicants for citizenship to have ‘good moral character,’ and largely defines that term through a list of unlawful or unethical behaviors”).

<sup>63</sup> 8 U.S.C. § 1101(f)(6) (2016).

<sup>64</sup> 18 U.S.C. § 1425(b).

<sup>65</sup> 8 U.S.C. § 1451(a).

<sup>66</sup> See Anthony D. Bianco, et al., *Civil Denaturalization: Safeguarding the Integrity of U.S. Citizenship*, U.S. ATTORNEYS’ BULL., July 2017, at 12.

<sup>67</sup> See *Berger v. United States*, 295 U.S. 78, 88 (1935) (“[The federal prosecutor] may prosecute with earnestness and vigor—indeed, he should do so. But, while he may strike hard blows, he is not at liberty to strike foul ones. It is as much his duty to refrain from improper methods calculated to produce a wrongful conviction as it is to use every legitimate means to bring about a just one.”).

<sup>68</sup> *Maslenjak v. United States*, 2017 WL 1495528 (U.S.), 55 (U.S. Oral. Arg., 2017).

in which OIL-DCS or HRSP can be of assistance in addressing the causation standard set forth in *Maslenjak*, please contact any of the authors or email [denaturalization@usdoj.gov](mailto:denaturalization@usdoj.gov).

## ABOUT THE AUTHORS

□ **Timothy M. Belsan** serves as the Deputy Chief of the Office of Immigration Litigation's District Court Section's National Security and Affirmative Litigation Unit. In that role, he oversees the office's denaturalization practice and is a frequent speaker and lecturer on the topic. He also has extensive experience in the areas of class action defense, justiciability doctrines, and habeas challenges to detention, and is a recipient of the Attorney General's Distinguished Service Award. He previously served as a Special Assistant United States Attorney in the Eastern District of Virginia's Criminal Division. Prior to joining the Department, he clerked for the Honorable Deanell Reece Tacha, former chief judge of the U.S. Court of Appeals for the Tenth Circuit, and served as an adjunct professor of law at Washburn University School of Law.

□ **Aram A. Gavoor** serves as Senior Counsel for National Security with the National Security and Affirmative Litigation Unit in the Office of Immigration Litigation's District Court Section. In his spare time, he is a Visiting Associate Professor of Law at The George Washington University Law School, where he teaches Administrative Law, Federal Courts, and Government Lawyering, catering principally to evening students. He has published scholarly works on constitutional, administrative, and immigration issues in a number of law reviews and has received awards in recognition of his Department and academic accomplishments.

□ **Joseph A. Marutollo** serves as an Assistant United States Attorney and Chief of Immigration Litigation at the U.S. Attorney's Office for the Eastern District of New York. As Chief of Immigration Litigation, he oversees his office's extensive civil immigration practice, which includes Administrative Procedure Act cases, class action litigation, and denaturalization actions. Prior to joining the U.S. Attorney's Office, he served as an Assistant Corporation Counsel at the New York City Law Department, where he worked in the Special Federal Litigation Division and represented the New York City Police Department in federal class action lawsuits.

Page Intentionally Left Blank

# International Parental Kidnapping: An Overview of Federal Resources to Assist Your Investigation and Prosecution

*Jennifer Toritto Leonardo*  
*Senior Trial Attorney*  
*Child Exploitation and Obscenity Section*  
*Criminal Division*

## I. Introduction

Every day, children in the United States are wrongfully removed from the United States or retained outside of the United States in violation of the parental rights of the left-behind parent or other person exercising parental rights. According to the State Department in its 2016 Annual Report on International Parental Child Abduction, more than 600 children were abducted by a parent from the United States to another country.<sup>1</sup> In its 2017 Report to Congress, the State Department reported that in 2016, 230 children abducted from the United States by a parent were returned to the United States, while another 189 child abduction cases were resolved without a successful return of the child.<sup>2</sup>

In 1993, Congress passed the International Parental Kidnapping Crime Act (“IPKCA” or “the Act”), which created a federal international kidnapping offense, codified in 18 U.S.C. § 1204. At that time, the United States was already a party to the Hague Abduction Convention (“Convention” or “Hague Convention”) (discussed in more detail in Part III below). The IPKCA, state criminal parental kidnapping statutes, and the Hague Convention provide separate and parallel mechanisms for the criminal prosecution of offenders and the civil return of children unlawfully removed from the United States. This Article is intended to provide critical information including an overview of these applicable civil and legal remedies related to international parental kidnapping (or “IPK”), an introduction to available federal resources, and an explanation of important roles played by local law enforcement, the FBI, the State Department and the Department of Justice.

## II. The Federal Criminal Statute

International parental kidnapping is criminalized in 18 U.S.C. § 1204, which reads:

- (a) Whoever removes a child from the United States . . . or retains a child (who has been in the United States) outside the United States with intent to obstruct the lawful exercise of parental rights shall be fined under this title or imprisoned not more than 3 years, or both.
- (b) As used in this section—

---

<sup>1</sup> Department of State, Annual Report on International Child Abduction (2016) at 5.

<sup>2</sup> Department of State, Annual Report on International Child Abduction (2017) at 6. The State Department classifies cases “resolved” without the successful return of the child when the parents reach a voluntary arrangement for the child to remain outside of the U.S., the left-behind parent withdraws the application for return, the left-behind parent cannot not be located for more than a year, or the child passed away. Department of State, Annual Report on International Child Abduction (2017) at 7.

- (1) the term “child” means a person who has not attained the age of 16 years; and
- (2) the term “parental rights”, with respect to a child, means the right to physical custody of the child–
  - (A) whether joint or sole (and includes visiting rights); and
  - (B) whether arising by operation of law, court order, or legally binding agreement of the parties.
- (c) It shall be an affirmative defense under this section that–
  - (1) the defendant acted within the provisions of a valid court order granting the defendant legal custody or visitation rights and that order was obtained pursuant to the Uniform Child Custody Jurisdiction Act or the Uniform Child Custody Jurisdiction and Enforcement Act and was in effect at the time of the offense;
  - (2) the defendant was fleeing an incidence or pattern of domestic violence; or
  - (3) the defendant had physical custody of the child pursuant to a court order granting legal custody or visitation rights and failed to return the child as a result of circumstances beyond the defendant’s control, and the defendant notified or made reasonable attempts to notify the other parent or lawful custodian of the child of such circumstances within 24 hours after the visitation period had expired and returned the child as soon as possible.
- (d) This section does not detract from The Hague Convention on the Civil Aspects of International Parental Child Abduction, done at the The Hague on October 25, 1980.<sup>3</sup>

Right off the bat, there are a few important things to note. First, unlike many of our other federal child exploitation statutes, § 1204 defines a “child” for purposes of the statute as a person under the age of sixteen.<sup>4</sup> Additionally, application of the statute extends to any “person” who abducts a child in contravention of “parental rights,” and not just parents. Thus, there may be factual situations in which a grandparent, adoptive parent, or other person exercising “parental rights” may be in violation of the statute.

Unlike many State parental kidnapping laws, a court order outlining custodial rights is not required to establish a violation of the Federal IPK statute. Under the statute, “parental rights” include not only those rights outlined by a court order or other legally binding agreement between the parties, but also rights arising out of operation of law.<sup>5</sup> In the absence of any existing court order, “parental rights” are defined by the law of the State in which the child resided before leaving the United States.<sup>6</sup> Under the law of most States, both parents are presumed to have joint physical custody in the absence of any court order or agreement.

Finally, investigators and prosecutors should note that Section 1204 does not include a mechanism to demand the return of the child. In fact, by enacting section (d) of § 1204, Congress specifically signaled its intent that a criminal prosecution under this Section should not interfere with the Hague Convention, a civil mechanism by which a left-behind parent can seek the return of the child. Even in cases in which a defendant is successfully prosecuted and sentenced for international parental kidnapping, there is no certain mechanism by which a U.S. criminal court can order the return of a child located overseas.<sup>7</sup> Because of this limitation in Section 1204, prosecutors and investigators must carefully

---

<sup>3</sup> 18 U.S.C. § 1204.

<sup>4</sup> 18 U.S.C. § 1204 (b)(1).

<sup>5</sup> 18 U.S.C. § 1204 (b)(2).

<sup>6</sup> *United States v. Amer*, 110 F.3d 873, 878 (2d Cir. 1997); *United States v. Fazal-Ur-Raheman-Fazal*, 355 F.3d 40, 43 (1st Cir. 2004); *United States v. Alahmad*, 28 F. Supp. 2d 1273, 1274 (D. Colo. 1998).

<sup>7</sup> See Jacqueline D. Golub, *The International Parental Kidnapping Crime Act of 1993: The United States' Attempt to Get Our Children Back-How Is It Working?*, 24 *BROOK. J. INT'L L.* 797 (1999) (discussing *Amer*, 110 F.3d 873, and fact that court had no authority to enforce its condition of probation that defendant return the child to the U.S.).

consider the impact of a criminal prosecution on any efforts to secure the child's return to the United States, including not just whether, but when, to pursue charges.

### **III. The Hague Abduction Convention and the State Department's Role in an International Parental Kidnapping Investigation**

#### **A. The Convention**

The Hague Convention on the Civil Aspects of International Child Abduction<sup>8</sup> is a multilateral treaty which provides a civil mechanism by which left-behind parents<sup>9</sup> can pursue the return of their child to the United States. Parents, as civil petitioners, may file a request for the return of a child who “habitually resided” in the United States and was removed to or retained in another Hague Convention partner country in violation of the left-behind parent’s custodial rights.<sup>10</sup> Under the Convention, each partner country has a designated Central Authority to carry out specialized duties under the Convention. The duties of the Central Authority include helping to locate an abducted child; facilitating requests under the Convention for the return of an abducted child, and assisting with planning for the safe return of the abducted child.<sup>11</sup> The International Child Abduction Remedies Act, (“ICARA”) implements the Hague Convention in the United States.<sup>12</sup>

Any country party to the Convention may refuse to return a child to his or her “habitual residence” if the taking parent successfully proves one of the limited defenses listed in the Convention. For example, if a petition for return is filed more than one year after a child is abducted or retained, and the taking parent can prove the child is well-settled in the new environment, a court may refuse to return the child. Additionally, a child may not be returned if there is grave risk that the child would be exposed to physical or psychological harm or otherwise placed in an intolerable situation in his or her country of habitual residence; if the child objects to his or her return and has reached an “age or degree of maturity” at which “it is appropriate to take account of its views”;<sup>13</sup> or if the child’s return would violate the fundamental principles of human rights and freedoms of the country where the child is being held.<sup>14</sup> As of 2016, the Convention is in force between the United States and seventy-five other countries. For a complete list of signatory countries and more information related to The Hague Convention, go to the State Department Website.

---

<sup>8</sup> The Hague Convention on the Civil Aspects of International Child Abduction, Oct. 25, 1980, T.I.A.A. No. 11,670, 1343 U.N.T.S. 89, *reprinted in* 51 FR 10494-01 (Mar. 26 1989) Abduction (“Hague Abduction Convention” or “Convention”).

<sup>9</sup> Neither Section 1204 nor the Hague Convention uses the term “left behind parent.” This Article uses the term to reference any person exercising “parental rights” under Section 1204 or “custodial rights” under the Hague Convention.

<sup>10</sup> The Hague Convention uses the term “rights of custody” rather than “parental rights.” These rights refer to “rights relating to the care of the child and, in particular, the right to determine the child’s place of residence.” Hague Convention *supra* Article 5.

<sup>11</sup> *See* Hague Convention *supra* Article 7.

<sup>12</sup> 42 U.S.C. §§ 11601-11611 (2000), *recodified at* 22 U.S.C.A. §§ 9001-9011 (2014).

<sup>13</sup> Hague Convention *supra* Article 13.

<sup>14</sup> *Id.* *supra* Article 20.

## **B. Role of the State Department Under the Hague Abduction Convention and Assistance Offered to Left Behind Parents**

The U.S. Department of State's Bureau of Consular Affairs, Office of Children's Issues ("CI") is designated as the U.S. Central Authority under the Hague Convention.<sup>15</sup> CI performs the following functions: promotes and strengthens the Convention in the United States and abroad; manages relationships and communication between left-behind parents, foreign governments, and other stakeholders; provides parents with information and resources available to them in the foreign country; monitors the Hague judicial process and updates parents on this process; works with U.S. embassies and consulates abroad, foreign central authorities, and U.S. law enforcement authorities to locate abducted children; and facilitates requests to DOJ's Office for Victims of Crime (OVC) to disperse travel assistance funds for both the child and left-behind parent when needed.<sup>16</sup>

In addition to providing invaluable services to left-behind parents pursuing a Convention petition, the State Department also serves as the left-behind parent's point of contact in abduction cases in which the offender and child are located in a non-Hague partner country. In this situation, CI can provide the parent with information on the country in which the child is located and discuss possible resources to help assist the parent in efforts to return the child to the United States. CI can also facilitate the parent's communication with other U.S. government agencies and non-governmental organizations that may be able to assist the parent.<sup>17</sup>

When speaking with a left-behind parent about how the State Department can help, investigators and prosecutors should understand that the State Department cannot provide legal guidance to a parent or act as a parent's legal representative; take possession of a child abducted by a parent; place a child into custody at the U.S. embassy; or assist U.S.-based child recovery services in locating and seizing the child. For more information about CI's role and contact information, go to the State Department OCI Website.

## **C. How the State Department Can Assist Law Enforcement**

In addition to helping left-behind parents, CI works regularly with law enforcement to help provide technical assistance and advice in IPK investigations. For example, CI may be able to facilitate the sharing of important passport information on children and abducting parents; coordinate with consular officers overseas to expeditiously issue U.S. travel documents when appropriate; ask the U.S. Embassy or consulate abroad to verify entry of a taking parent or child into a country; ask for a welfare check on a child; and provide country specific information to law enforcement.<sup>18</sup>

Additionally, CI's Prevention Branch administers the Children's Passport Issuance Alert Program ("CPIAP"), an important State Department tool to prevent international parental child abduction. Under U.S. law, any person under the age of sixteen must apply for a passport in person, and the passport applicant must submit documentation that lists the parent or parents or legal guardian(s) of the child applying for a passport. With the help of the CI Prevention Branch, parents may enroll their U.S. citizen children under the age of eighteen in CPIAP. If a passport application is submitted for a child who is

---

<sup>15</sup> See 42 U.S.C. §§ 11601-11610.

<sup>16</sup> *Id.* The National Center for Missing and Exploited Children ("NCMEC") and CI have established a cooperative agreement with OVC known as the "Victim Reunification Travel Program" which provides OVC funding to left behind parents covering transportation expenses required to attend foreign court proceedings, translation of documents related to court hearings, and other travel costs associated with the reunification process. Since 1996, NCMEC's Family Advocacy Division manages this program and coordinates with OVC and DOJ's Office of Juvenile Justice and Delinquency Prevention ("OJJDP") to appropriate disbursements under this program. For more information see NCMEC and OVC Victim Services.

<sup>17</sup> *Id.*

<sup>18</sup> See State Department: Abduction Prevention Website.

enrolled in CPIAP, the CI Prevention Branch works to alert the enrolling parent(s) to verify whether the two-parent consent requirement for passports has been met.<sup>19</sup>

CI's Prevention Branch also assists law enforcement responding to an abduction-in-progress by working with the Department of Homeland Security Customs and Border Patrol ("DHS CBP"). CI's Prevention Branch maintains a 24/7 duty program, as does the State Department's Overseas Citizen Services for the public and law enforcement; provides prevention information to the public; and along with CI's Abduction Branches, conducts training on international parental abduction prevention to both State Department and external audiences. For more information, go to the State Department Abduction Prevention Website.

## IV. The FBI's Role in an IPK Investigation

Under the IPKCA, the FBI is the law enforcement agency tasked with investigating IPK cases. The FBI can take steps to stop abductions in progress and can coordinate the international law enforcement response when abductors have reached their foreign destinations. Both local and federal law enforcement may request information and assistance from foreign law enforcement by working with the FBI's Legal Attaché, otherwise known as the Legat. Legats are stationed at U.S. Embassies and may request assistance from the relevant country's law enforcement to locate and/or confirm the location of either the abductor or child. As discussed below, the FBI also assists prosecutors in obtaining an Unlawful Flight to Avoid Prosecution ("UFAP") warrant under the Fugitive Felon Act.<sup>20</sup>

### A. What is a UFAP Warrant

In addition to the federal IPK offense, almost every State has a statute which criminalizes international parental kidnapping. Depending on the circumstances (including the fact that extradition may be more readily obtained under a state statute, depending on the foreign country involved and the applicable U.S. extradition treaty with that country), law enforcement and prosecutors may wish to pursue local charges rather than prosecute the offender under the federal statute. Either way, extradition is the formal process by which a person found in one country is surrendered to another country for trial or punishment.<sup>21</sup> Law enforcement and prosecutors pursuing local charges may still wish to secure the assistance of federal authorities in locating and apprehending foreign fugitives. In order to obtain this assistance, prosecutors and law enforcement personnel must rely on a UFAP warrant, as authorized by the Fugitive Felon Act, 18 U.S.C. § 1073.<sup>22</sup> The primary purpose of the Fugitive Felon Act is to assist states in apprehending fugitives from state justice.<sup>23</sup>

Congress explicitly stated in the Parental Kidnapping Prevention Act of 1980 ("PKPA") that cases involving fugitives of an international parental kidnapping are appropriately covered by the UFAP process. Pursuant to this process, a local or state prosecutor requests a UFAP warrant from a federal prosecutor or the FBI, after verifying that a state or local felony warrant for the offender already exists and that the state or local prosecutor agrees to extradite the fugitive for prosecution.<sup>24</sup> Once this information is verified, a federal prosecutor files a complaint charging the fugitive with a violation of 18 U.S.C. § 1073 based on probable cause that the fugitive has fled the jurisdiction of the State to avoid prosecution or confinement.

---

<sup>19</sup> See Children's Passport Issuance Alert Page.

<sup>20</sup> See FBI Violent Crimes Against Children Website.

<sup>21</sup> See generally, U.S. ATTORNEY'S MANUAL (USAM) 9-15; FED. CRIM. RES. MANUAL 602.

<sup>22</sup> See also, FED. CRIM. RES. MANUAL 1780.

<sup>23</sup> *Id.*

<sup>24</sup> USAM 9-15.1000.

Once the local prosecutor obtains a UFAP warrant, the FBI is able to access national and international resources to assist local law enforcement in locating and apprehending the offender. If agents discover that the abductor is abroad, they may request the assistance of foreign law enforcement through the FBI's Legat.

## V. INTERPOL Notices: How They Can Help Your Investigation

Investigators and prosecutors faced with an IPK offender who has left the country should be aware of other tools at their disposal to help locate both offender and victim. International Notices published by INTERPOL and other INTERPOL resources may help this process.

The International Criminal Police Organization ("INTERPOL") is the world's largest international police organization. INTERPOL's aim is to facilitate police cooperation and provide a communication system and various other resources to assist the criminal investigative and humanitarian efforts of law enforcement officials.<sup>25</sup> Participation by countries in INTERPOL is voluntary, and INTERPOL itself has no international jurisdiction or agents. Each INTERPOL member country maintains a National Central Bureau ("NCB") that serves as that country's point of contact for all INTERPOL matters and for communication with NCBs in other INTERPOL member countries. Interpol Washington, the U.S. National Central Bureau (USNCB), a component of the U.S. Department of Justice, is the United States' representative to INTERPOL.<sup>26</sup> When an international parental kidnapping case takes place, law enforcement authorities can contact the USNCB to seek guidance on the use of INTERPOL's resources in pursuing their case.<sup>27</sup>

INTERPOL Notices are international requests for assistance or alerts allowing police in member countries to share crime-related information.<sup>28</sup> For example, an INTERPOL "Red Notice" is an international wanted notice that provides information on the identification of a fugitive who is the subject of an arrest warrant and is wanted for prosecution or to serve a sentence for a serious offense. Red Notices are published by INTERPOL at the request of member countries in order to seek the location of fugitives for the purpose of extradition or other lawful return. Once published, each INTERPOL member country determines what effect to give a Red Notice within its jurisdiction according to its national law and practice. At a minimum, a country receiving a Red Notice issued by another country is expected to enter the Red Notice and information about its subject into its national lookout databases, and to expeditiously contact the requesting country should the fugitive be located in its territory. Approximately one third of INTERPOL's 192 member countries consider a Red Notice to be the equivalent of a provisional arrest request for the purpose of extradition and will detain the subject of a Red Notice depending on circumstances such as the relationship between the countries involved, whether an extradition treaty is applicable, the type of offense involved, and risk of flight. Please note that a Red Notice is a firm commitment by the requesting country to follow up any notification of location or arrest with an extradition request when possible and appropriate. Further, Red Notices relate to the location, arrest and return of fugitives, and are not intended to address the location or return of a kidnapped child.

Alternatives to Red Notices include: Blue Notices, which are published to obtain information concerning the identity, location, or illegal activities of a person of interest in a criminal investigation (including defendants, suspects, witnesses, and victims); and Diffusions, which are formatted messages requesting assistance for purposes similar to the various types of INTERPOL notices, including seeking to locate wanted and missing persons. Diffusions are sent directly by NCBs to one or many countries and the assistance requested can be tailored to the particular circumstances of a case.

---

<sup>25</sup> See Interpol Website.

<sup>26</sup> See 22 U.S.C § 263a, and 28 C.F.R. § 0.34.

<sup>27</sup> See Interpol-Washington.

<sup>28</sup> See Interpol Website Notices.

Finally, INTERPOL Yellow Notices are published in order to locate a missing person (adult or minor, including kidnapping victims) or to identify a person who is unable to identify him or herself. Yellow Notices are often issued in IPK cases in addition to Red Notices on the parental abductors.

## VI. How OIA and CEOS Can Help

DOJ's Office of International Affairs (OIA) provides information and advice to federal and state prosecutors about the procedure for requesting extradition from abroad, and advises and provides support to federal prosecutors handling foreign extradition requests for fugitives found in the United States.<sup>29</sup> OIA also initiates all requests for provisional arrests of fugitives pursuant to extradition treaties.<sup>30</sup> Because every extradition treaty is negotiated separately, prosecutors considering an IPK charge against an offender who is not located in the United States should contact OIA at the onset of any investigation to discuss extradition or other means to return an offender to the United States. More information about OIA can be found at the OIA website.

Finally, Trial Attorney's with DOJ's Child Exploitation and Obscenity Section ("CEOS") work in partnership with the ninety-four U.S. Attorney's Offices to investigate and prosecute defendants who have violated federal child sexual exploitation laws, including violations of the federal IPK statute. CEOS also provides advice and litigation support to other federal prosecutors regarding prosecutions under Section 1204, and conducts training for prosecutors, law enforcement personnel, and others on IPK matters. Information about how CEOS can assist you in your IPK investigation or prosecution can be found at the CEOS Website.

## VII. Conclusion

When investigators and prosecutors are faced with a potential IPK case, it is important to consider all of the available federal resources discussed above to aid in the investigation. Prosecutors must also consider the unique challenges and considerations in an IPK case before initiating a prosecution. Investigators and prosecutors should contact the FBI, the State Department, and DOJ's OIA and CEOS to discuss any issues raised in this Article and to seek assistance.

### ABOUT THE AUTHOR

**Jennifer Toritto Leonardo** is a Senior Trial Attorney with the Criminal Division's Child Exploitation and Obscenity Section (CEOS). Jennifer started her legal career as an Assistant District Attorney at the Manhattan District Attorney's Office where she specialized in prosecuting domestic violence crimes, including rape, assault, and child abuse. She has received the Assistant Attorney General's Distinguished Service Award, and twice received the Assistant Attorney General's Award for Outstanding Advocacy for Protecting Citizens from Online Crime.

*Jennifer would like to thank the Office of General Counsel, Interpol Washington; Sean Watson; Terry Schubert, Trial Attorney with the Office of International Affairs; and Joshua Wilson, Supervisory Special Agent with the FBI for their contributions to this article.*

---

<sup>29</sup> See USAM 9-15.210.

<sup>30</sup> *Id.* at 9-15.230.

Page Intentionally Left Blank

# Protecting Law Enforcement Peer-to-Peer Investigations

*Jeffrey H. Zeeman*  
*Trial Attorney*  
*Office of Enforcement Operations*

*Joanne C. Pasquarelli*  
*Assistant General Counsel*  
*FBI Office of the General Counsel*

Federal, state and local law enforcement agencies have developed and routinely deploy proprietary software tools to identify thousands of offenders who exploit children by sharing child pornography over peer-to-peer (P2P) file sharing networks. Those tools, however, are increasingly targeted by defendants through overbroad discovery requests, often bearing little relationship to any cognizable legal defense to the charged conduct. While the Department of Justice supports full compliance with all discovery obligations imposed by law, those obligations generally do not require disclosure of sensitive information regarding law enforcement techniques which, if exposed, would threaten the viability of future investigations. Accordingly, the Department has drawn an effective line between disclosure of the information required for defendants to prepare their defense and protection of sensitive information germane to the continued effectiveness of undercover law enforcement techniques. Recent court rulings have thoroughly examined these issues for P2P investigative tools, and generally agree that the balance struck by the Department is appropriate. As law enforcement tools advance and expand to investigations of other online technologies employed to commit criminal offenses, the importance of protecting sensitive information related to online investigative tools increases. This article provides an overview of the recent case law addressing this issue and offers strategies for protecting P2P tools during discovery in federal prosecutions of child pornography offenders.

## I. Background on Law Enforcement P2P Tools

Law enforcement agencies have developed a number of tools used to ascertain the IP addresses responsible for sharing child pornography files via the most frequently utilized P2P networks. In 2006, the FBI first developed its eP2P tool, which enabled investigation of those sharing child exploitation images shared through the Gnutella P2P network. Later, the FBI began employing the RoundUp suite of tools to investigate child exploitation occurring on the Gnutella, eMule, Ares, and BitTorrent networks, among others. Other law enforcement and private sector entities have developed similar P2P tools, including Shareaza LE, Torrential Downpour and TLO.

Each tool is specifically designed for a particular P2P network/s, with marginally different functionality. The RoundUp suite of P2P tools all share these common characteristics:

- The tools operate within the protocol of the existing P2P network, allowing law enforcement agents to identify P2P users sharing child pornography with the public. When a law enforcement agent submits a request to the P2P network seeking to download files of known child pornography, the network identifies which IP addresses are sharing these files with the public.
- The tools report the IP addresses identified to be sharing known child pornography files to a centralized database as a means of sharing investigative leads and allowing agents to focus on

suspect IP addresses located within their jurisdiction. The IP addresses that are known to be sharing child pornography with the public are often referred to as “download candidates”.

- The tools enable law enforcement agents to download publicly-shared child pornography files from a single IP address. Unlike standard P2P programs, which simultaneously download different pieces of the same file from different users to speed up the downloading process, the law enforcement version only downloads images from a single computer, otherwise called a single source, enabling the law enforcement agent to download the entire image from one target.
- The tools may or may not allow for the *appearance* of file sharing, but none of the tools enable law enforcement to actually share contraband files via a P2P network.
- Critically, none of the tools allow law enforcement to obtain information from a user’s computer that the user is not publicly sharing via the P2P network. As such, the tools lack the ability to invade constitutionally protected private spaces.

Typically, law enforcement can articulate probable cause to support a search warrant for a residence or other location by identifying associated IP addresses sharing child pornography with the public. Electronic storage materials seized during the execution of the search warrant are then analyzed forensically, in most cases revealing evidence of possession, distribution and/or production of child pornography.

## II. Recent Case Law

In recent years, federal courts have published a number of decisions addressing defense requests for disclosure of either an executable copy of proprietary law enforcement P2P software, or a copy of the software’s source code. In nearly every case, courts denied defendants’ discovery requests as overbroad under FED. R. CRIM. P. 16, protected by the law enforcement privilege, or on both grounds.<sup>1</sup> For reasons discussed below, the primary case in which a court suggested that disclosure of a tool’s source code may be warranted is readily distinguishable from the bulk of P2P investigations because of its unusual facts and procedural history.

### A. Courts Throughout the Country Have Denied Defense Requests for the Source Code of Proprietary Investigative Tools

Two federal appellate courts and many district courts have ruled that the source code of law enforcement P2P tools is not discoverable. Courts have grounded those rulings in findings that: (1) discovery requests were overbroad under FED. R. CRIM. P. 16, (2) defendants failed to overcome the protection afforded by the law enforcement privilege, or both. The first court to address a defense request for disclosure of the source code of a law enforcement P2P tool was *United States v. Chiaradio*, where the defendant moved to compel production of the eP2P source code, arguing it was: material to preparing his defense;<sup>2</sup> necessary as a report of a scientific exam;<sup>3</sup> necessary as a written summary of proposed government experts;<sup>4</sup> and necessary to challenge the reliability of government experts under *Daubert*.<sup>5</sup> The Court of Appeals for the First Circuit dismissed the second and third arguments based on Rule 16(a)(1)(F)&(G) (scientific exam and written summary of experts) as “patently meritless” before

---

<sup>1</sup> General background on the scope of FED. R. CRIM. P. 16 and the law enforcement privilege is provided at pp. 7-9, *infra*.

<sup>2</sup> FED. R. CRIM. P. 16 (a)(1)(E)(i).

<sup>3</sup> FED. R. CRIM. P. 16 (a)(1)(F).

<sup>4</sup> FED. R. CRIM. P. 16 (a)(1)(G).

<sup>5</sup> *United States v. Chiaradio*, 684 F.3d 265, 277 (1st Cir. 2012).

addressing whether the district court had abused its discretion in rejecting defendant's Rule 16(a)(1)(E) argument.<sup>6</sup>

The Court of Appeals for the First Circuit declined to rule on the materiality of the source code under Rule 16(a)(1)(E), holding that such a ruling was unnecessary in light of the defendant's failure to demonstrate any possible prejudice to him from nondisclosure.<sup>7</sup> The government argued that, in light of the evidence produced to the defendant, he had failed to demonstrate need for the source code to support a defense that the government had downloaded some portions of the child pornography file at issue from other P2P users. Specifically, the government produced the PCAP (packet capture) file, which is a recording of the entire download of a shared file to the undercover agent's computer using the eP2P tool, and a copy of the FBI guide detailing how to reconstruct an eP2P session manually using only the PCAP file and publicly available programs. At the hearing on the motion to compel, the government presented an expert witness who described the functionality of eP2P and provided a live demonstration of the file capture process, demonstrating the methodology for verifying that the entire image downloaded by the undercover agent originated from the defendant's computer. The defendant neither contradicted nor cast the slightest doubt upon this testimony.<sup>8</sup> After reviewing this evidence, the Court of Appeals for the First Circuit concluded that the government's disclosure of the PCAP file and specific instructions on how to recompile the downloaded image from that file "makes it pellucid that the forbidden files were located on the defendant's computers."<sup>9</sup>

A particularly strong case for the government is *United States v. Pirosko* in which the Court of Appeals for the Sixth Circuit affirmed the district court's denial of a motion to compel disclosure of "the law enforcement tools and records" (there, ShareazaLE) used to ascertain that the defendant's computer was sharing child pornography with the public.<sup>10</sup> The government objected on both Rule 16 materiality and law enforcement privilege grounds, arguing that granting the motion to compel "would compromise the integrity of its surveillance system and would frustrate future surveillance efforts."<sup>11</sup> The Court of Appeals for the Sixth Circuit endorsed both of the government's arguments. The court ruled in the government's favor on materiality grounds for two reasons: first, because the requested law enforcement tool was pertinent only to whether the defendant distributed child pornography, which was not required to prove the charged receipt offense, and second, because the government had introduced sufficient evidence to prove that the defendant had distributed child pornography, regardless of the viability of a speculative defense theory grounded in the operation of the undercover tool.<sup>12</sup>

Of particular import is *Pirosko*'s analysis of the law enforcement privilege, as the Court of Appeals for the Sixth Circuit agreed with the district court's application of a balancing approach, weighing the government's investigative concerns against the needs articulated by the defendant.<sup>13</sup> Employing this approach still requires the "government's investigative methods to be reliable, both for individual defendants . . . and for the public at large."<sup>14</sup> But, it is "important for the defendant to produce some evidence of *government wrongdoing*" in order to overcome the law enforcement privilege.<sup>15</sup> This test, if widely adopted, should foreclose wholly speculative fishing expeditions for the source code of P2P investigative tools, which is a common defense approach in P2P-based child pornography cases. After all,

---

<sup>6</sup> *Id.* at 276, n. 4.

<sup>7</sup> *Id.* at 277.

<sup>8</sup> *Id.*

<sup>9</sup> *Id.*

<sup>10</sup> *United States v. Pirosko*, 787 F.3d 358, 362 (6th Cir. 2015).

<sup>11</sup> *Id.* at 365.

<sup>12</sup> *Id.* at 367-69.

<sup>13</sup> *Id.* at 365.

<sup>14</sup> *Id.* at 366.

<sup>15</sup> *Id.* at 366 (emphasis supplied).

through a careful explanation of how P2P tools function, the government should in every case be able to demonstrate that any assertion of government wrongdoing is unfounded—because none of the tools provide investigators with access to *any* contraband file, save for those that offenders have made available to the general public.

In addition to these two favorable appellate decisions, several district court opinions have carefully considered complex discovery issues in P2P cases before ultimately ruling in the government’s favor by protecting law enforcement’s P2P tools. Most recently, in the Eastern District of Missouri, the court issued a lengthy and technically detailed opinion denying the defendant’s motion to compel disclosure of the source code, software, and manuals for Torrential Downpour, which is used to investigate child pornography shared through the BitTorrent file sharing network.<sup>16</sup> There, a state law enforcement officer utilized Torrential Downpour software to download files containing child pornography from an IP address later identified to be associated with the defendant’s residence. Four months later, a search warrant executed at that residence yielded numerous electronic storage devices containing child pornography. Based on the unsurprising fact that the particular files downloaded by law enforcement were not located in the defendant’s shared folder at the time of seizure, the defendant asserted that Torrential Downpour had illegally searched private folders on his computer without a warrant.

To support this argument, the defendant sought disclosure of the Torrential Downpour source code, manuals, and validation testing report, arguing that such disclosure was necessary to: prepare his defense against the charges based upon the downloaded files; determine if the downloads constituted an unlawful search; and prepare for the cross-examination of the state officer that conducted the downloads. In response, the government highlighted the extensive information already produced to the defense (including the logs collected during the downloads from the defendant’s computer and a live demonstration of the Torrential Downpour software) in arguing that the requested information was not material to the defendant’s case and, further, was protected by the law enforcement privilege. The court denied the motion to compel disclosure after finding that the defendant failed to demonstrate that the requested information was material to his defense.<sup>17</sup> Specifically, “nothing in the pending receipt-of-child-pornography charge reveal[ed] that the charge [was] based, to any extent, on materials downloaded from Defendant’s computer while [the investigating agent] used Torrential Downpour.”<sup>18</sup> The court proceeded to specifically reject each aspect of the defendant’s claimed need. Of particular note, in dismissing the defendant’s claim that the requested disclosures were necessary to explore a Fourth Amendment argument, the court held that the defendant’s expert submissions failed to evidence intrusion by the undercover officer into non-shared information on the defendant’s computer.<sup>19</sup> Accordingly, the defendant had no Fourth Amendment basis to object to the government’s retrieval of his publicly shared files, and the requested disclosures were not material to his defense.<sup>20</sup> In addition, the court also ruled in the government’s favor on law enforcement privilege grounds, holding that the defendant had failed to establish through his expert declaration a need for privileged information that outweighed the public’s interest in nondisclosure.<sup>21</sup>

Other district courts have likewise consistently denied requests for production of P2P tool source code either on materiality grounds, law enforcement privilege grounds, or both. In *United States v. Blouin*, the defendant moved to compel not only the source code for the P2P tool, but also law enforcement’s database of hash values associated with known child pornography, and the “download

---

<sup>16</sup> See *United States v. Hoeffener*, No. 4:16CR00374 JAR/PLC, 2017 WL 3676141 (E.D. Mo. Aug. 25, 2017).

<sup>17</sup> *Id.* at 13.

<sup>18</sup> *Id.*

<sup>19</sup> *Id.* at 17.

<sup>20</sup> *Id.*

<sup>21</sup> *Id.* at 19.

candidate” database.<sup>22</sup> The court denied these last two requests as overbroad, instead ordering disclosure of only the limited hash values associated with the files actually downloaded from the defendant’s computer.<sup>23</sup> With respect to the source code request, the court adopted the *Pirosko* court’s reasoning, holding that the defendant had failed to meet the Rule 16 standard for disclosure because he failed to produce any evidence of government wrongdoing.<sup>24</sup> Furthermore, the court was persuaded that, like in *Pirosko*, granting the defendant’s discovery request would compromise the integrity of the government’s surveillance system and frustrate future surveillance efforts.<sup>25</sup> In *United States v. Feldman*, the district court affirmed a magistrate judge’s denial of a motion to compel production of the RoundUp program, its manual, and protocols, noting that the “defendant fail[ed] to identify any specific defenses that discovery of the RoundUp materials could help him develop.”<sup>26</sup> Finally, in *United States v. Brashear*, the district court dismissed the defendant’s attempt to compel disclosure of RoundUp’s source code, reasoning that it was not relevant to the defendant’s argument that the program violated the Fourth Amendment.<sup>27</sup> “[T]he RoundUp program only accesses files shared through the file sharing network [and by] sharing files with the network, Brashear essentially shared those files with the public. He had no reasonable expectation of privacy over the files shared with Gnutella and, therefore, the use of the RoundUp program could not have violated his Fourth Amendment rights.”<sup>28</sup>

## **B. The *Budziak* Outlier: Unusual Facts and a Limited Holding**

*United States v. Budziak* is the lone published decision in which a federal court has held that the source code of the P2P tool was relevant to the defense under Rule 16.<sup>29</sup> *Budziak*, however, featured unusual facts and a convoluted procedural history, including two appellate rulings sandwiched around a remand, limiting the impact of its holding both within the Ninth Circuit and as persuasive authority elsewhere. Indeed, as discussed in detail below, multiple courts—including a district court within the Ninth Circuit—have denied defense requests for source code disclosures notwithstanding a defendant’s reliance on *Budziak*. Nevertheless, because every defendant seeking discovery of a P2P tool’s source code is sure to cite to *Budziak*, it is important for prosecutors to understand the case and be prepared to distinguish its unusual facts.

In *Budziak*, the defendant moved to compel the government to produce technical specifications, all documentation pertaining to eP2P, and an installable copy of that program, arguing that he needed these documents to support his defense that the images on his computer were obtained from various P2P users or sources, and then reassembled.<sup>30</sup> The district court denied the motion to compel, noting that the government had demonstrated, via computer logs, screen shots, and supporting declarations, that the source code would not provide the defendant the information he needs, and therefore he failed to satisfy Rule 16’s materiality requirement.<sup>31</sup> Although the court noted that the government had also raised the law

---

<sup>22</sup> *United States v. Blouin*, No. CR16-307 TSZ, 2017 WL 2573993 (W.D. Wash. June 14, 2017).

<sup>23</sup> *Id.* at 2-3. Beyond being overbroad, this type of request is problematic for a number of other reasons. Sharing law enforcement’s entire database of hash values associated with known child pornography files would (1) provide collectors with a roadmap to evade law enforcement by only sharing files excluded from the database, and (2) would also allow child pornography collectors to gain valuable information about files which may be missing from their collections, and potentially encourage them to seek out those files specifically.

<sup>24</sup> *Id.* at 3.

<sup>25</sup> *Id.*

<sup>26</sup> *United States v. Feldman*, No. 13-CR-155, 2015 WL 248006, at 6-7 (E.D. Wis. Jan. 19, 2015).

<sup>27</sup> *United States v. Brashear*, No. 4:11-CR-0062, 2013 WL 6065326, at 2 (M.D. Pa. Nov. 18, 2013).

<sup>28</sup> *Id.* at 3.

<sup>29</sup> *United States v. Budziak*, 697 F.3d 1105, 1113 (9th Cir. 2012).

<sup>30</sup> *Id.* at 1111-12.

<sup>31</sup> *Id.* at 1112.

enforcement privilege, the court relied only upon Rule 16's materiality requirement in reaching its conclusion.<sup>32</sup>

Following his jury trial conviction for distribution and possession of child pornography, the defendant appealed to the Court of Appeals for the Ninth Circuit, which held that the district court abused its discretion when it denied the motion to compel, and remanded the case for further consideration.<sup>33</sup> In so doing, the court emphasized that Budziak "identified specific defenses to the distribution charge that discovery on the EP2P program could potentially help him develop" by producing "evidence suggesting that the FBI may have only downloaded fragments of child pornography files from his 'incomplete' folder, making it 'more likely' that he did not knowingly distribute any complete child pornography files to [the undercover agents]," as well as "evidence suggesting that the FBI agents could have used the EP2P software to override his sharing settings."<sup>34</sup> "Given that the distribution charge against Budziak was premised on the FBI's use of the EP2P program to download files from him, it is logical to conclude that the functions of the program were relevant to his defense . . . In cases where the defendant has demonstrated materiality, the district court should not merely defer to government assertions that discovery would be fruitless. While we have no reason to doubt the government's good faith in such matters, criminal defendants should not have to rely solely on the government's word that further discovery is unnecessary. This is especially so where, as here, a charge against the defendant is predicated largely on computer software functioning in the manner described by the government, and the government is the only party with access to that software."<sup>35</sup> Accordingly, the Court of Appeals for the Ninth Circuit remanded the case to the district court for a determination of whether the eP2P materials requested by Budziak in fact contained, or would have led to, information that might have altered the verdict.<sup>36</sup>

When rebutting a defendant's reliance on *Budziak*, prosecutors should emphasize the following, in addition to any other case-specific arguments that may be applicable. First, Budziak stipulated to all elements of the offense save for the distribution element, making the eP2P-derived evidence atypically central to the government's burden of proof.<sup>37</sup> Second, neither the district court nor the Court of Appeals for the Ninth Circuit considered the government's law enforcement privilege argument, an argument that

---

<sup>32</sup> *Id.* at 1113.

<sup>33</sup> *Id.*

<sup>34</sup> *Id.* at 1112.

<sup>35</sup> *Id.* at 1112-13.

<sup>36</sup> In *Budziak*, following remand, the district court ruled that defendant was entitled to examine the source code of the version of eP2P used in the investigation, but it did not order the government to produce a copy of that code to defense. Instead, the court mandated that the defense team be granted access to the source code, at a government facility, under a protective order designed to protect the code from further dissemination. The government then disclosed that it had lost or destroyed the source code of the particular version of the eP2P program (which was by then obsolete) used to investigate the defendant. *United States v. Budziak*, 612 F. App'x 882, 884 (9th Cir. 2015) (*Budziak II*) (unpublished disposition). In light of the government's disclosure, defendant moved for discovery sanctions under FED. R. CRIM. P. 16(d)(2), requesting dismissal of the indictment or suppression of any eP2P-related evidence. *Id.* The district court denied defendant's motion for discovery remedies and reinstated defendant's possession of child pornography conviction; defendant appealed, arguing that because the government failed to turn over the source code, the district court had violated its mandate. *Id.* The Court of Appeals for the Ninth Circuit later affirmed the defendant's possession of child pornography conviction, noting that defendant "had not requested the source code in the earlier district court proceedings, and in fact specifically said its disclosure was not necessary." *Id.* In addition, the district court determined on remand that nondisclosure of the requested eP2P materials was harmless, and that defendant had failed to demonstrate prejudice from that nondisclosure despite ample opportunity to do so. *Id.* at 884-85.

<sup>37</sup> The only contested charge against Budziak was distribution of child pornography, which was based solely upon the downloads conducted by the FBI using the eP2P tool. This meant that "[m]uch of the evidence the prosecution presented at trial was devoted to describing EP2P and the FBI's use of the program." *Budziak*, 697 F.3d at 1112.

has since proven dispositive in *Pirosko*, among other cases. Third, and critically, the defendant was able to make a detailed factual proffer to support his purported need for the requested materials—specifically, media reporting of an illicit backdoor which the defendant alleged would allow overriding of his file-sharing settings.<sup>38</sup> Fourth, even in *Budziak*, the Court of Appeals for the Ninth Circuit ultimately ruled following remand that nondisclosure of the requested eP2P materials was harmless in affirming the defendant’s child pornography possession conviction.<sup>39</sup>

Indeed, other federal courts have generally had little difficulty distinguishing *Budziak* on these types of grounds. For example, in *Pirosko*, the Court of Appeals for the Sixth Circuit emphasized that the defendant had provided no evidence to undermine the government’s factual proffer describing how investigators legitimately downloaded child pornography from the defendant’s shared folders, in contrast with *Budziak*, where the defendant submitted evidence suggesting unlawful intrusions overriding the defendant’s sharing settings and downloads of fragments of child pornography from incomplete files.<sup>40</sup> The *Blouin* court, which was bound by *Budziak*, distinguished it on the same grounds, noting that “[d]efendant does not dispute that RoundUp eMule downloads only from a single source, and he does not allege that either eMule or Shareaza, like LimeWire, allows a user (or a connecting “peer,” e.g., a law enforcement agent) to modify the sharing settings.”<sup>41</sup> The *Hoeffener* court emphasized two key distinguishing factors: (1) the distribution charges against *Budziak* were primarily based upon the evidence collected by the eP2P tool, and (2) the additional evidence *Budziak* presented to support his defense theories.<sup>42</sup> Importantly, in all three of these cases, the courts suggested that, even had defendant satisfied his burden on materiality, the government’s invocation of the law enforcement privilege *still* would have proven dispositive.

### **III. Preparing for and Responding to Defense Discovery Requests: Best Practice Pointers**

#### **A. Avoiding Litigation Through Charging Decisions and Preemptive Disclosure**

In order to foreclose defense arguments that production of an investigative tool’s source code is required, the government should produce as much potentially relevant non-sensitive information at the outset of discovery as possible, including, for example, full and timely access to all materials seized from defendant; copies of all logs or other data captured by the program that pertains to a defendant’s P2P activities, including the PCAP file that proved dispositive in *Chiaradio*; written responses to interrogatories answering case-specific concerns about the tool’s functionality; in-person demonstrations of pertinent aspects of the tool’s functionality (e.g., a demonstration of a single-source download); expert declarations that address misinformed or outright deceptive defense claims about the tool’s functionality; and any specific forensic evidence that rebuts whatever argument the defendant claims necessitates review of the source code. In many cases, such voluminous disclosure is not required by FED. R. CRIM. P. 16 or by case law. Nevertheless, prosecutors may be able to resolve contentious discovery battles without litigation, and better position themselves for any prospective discovery litigation, by producing at the outset of discovery the non-law enforcement sensitive information related to the key functionality of the law enforcement tool and its deployment during the investigation in question. These types of disclosures and demonstrations are important not just for addressing misleading defense arguments, but also for generally educating judges, many of whom are not fluent in P2P technology and may not understand how

---

<sup>38</sup> The eP2P program is not, in fact, capable of exploiting any back door into an offender’s computer. *See* *United States v. Budziak*, N.D. Cal. Case No. 08-00284, Dkt #127-1, Declaration of Special Agent Michael Gordon.

<sup>39</sup> *Budziak II*, 612 F. App’x at 884-85.

<sup>40</sup> *Pirosko*, 787 F.3d at 365-66.

<sup>41</sup> *Blouin*, 2017 WL 2573993 at 3.

<sup>42</sup> *See* *Hoeffener* at 12.

law enforcement tools function, and in particular, that those tools are not capable of intruding into an offender's non-public files.

Note that investigators should only share information pertinent to the functionality of the specific law enforcement tool and capabilities utilized during the investigation of the offender seeking discovery. Information on the tool's other capabilities, including its employment in other investigations, should not be disclosed, because such information is irrelevant to the case-at-hand. The more comprehensive the initial disclosure of a tool's use in the investigation at issue, the more likely it is that a defendant, his counsel, and his forensic expert will understand the strength of the government's evidence. Enhancing the court's understanding of a tool's reliability and inability to intrude into privately maintained data, likewise, reduces the likelihood of an expansive discovery order premised on a misunderstanding of the scope of a tool's functionality. It is important in all cases to consult with those law enforcement personnel who manage the tool prior to disclosures illuminating its functionality, to ensure that sensitive information is not inadvertently disclosed.

In addition to producing evidence derived from the law enforcement tool itself, the government should make readily available to the defense team all forensic evidence seized from the offender. In many cases, defendants will attempt to justify requests for law enforcement-sensitive information by citing to a prospective defense that may be foreclosed upon thorough forensic examination of a defendant's seized computer. For example, if a defendant claims that a law enforcement tool was responsible for implanting child pornography on his computer, that defense can be tested by examining the defendant's computer for any evidence of intrusion (and of course, no scintilla of evidence supporting such a theory will ever be discovered).<sup>43</sup> If the defense declines to review the seized materials, yet still moves to compel production of sensitive law enforcement data, the government can persuasively argue that the defense team failed to examine the most pertinent evidence of wrongdoing prior to engaging in a speculative fishing expedition grounded in an incomplete understanding of the government's evidence.

As another avenue to limit the impact of adverse discovery rulings, prosecutors should (when consistent with local and Departmental charging policies) protect the integrity of a conviction by charging offenders with conduct that does not directly involve the undercover download. For example, prosecutors can charge counts of distribution grounded entirely in forensic evidence recovered from an offender's electronic storage devices. Additionally, prosecutors should in nearly every case be able to charge at least one count of receipt of child pornography—which offers the same penalty range as distribution, albeit typically resulting in a marginally lower guideline calculation—based entirely on evidence recovered during or after the execution of a search warrant. Courts, including *Budziak*, have consistently held that even when discovery of a P2P undercover tool may be relevant to a case, the scope of relevance is limited to distribution charges grounded in undercover downloads through the P2P tool in question. Ultimately, if the government charges a sufficiently broad scope of misconduct, a court is far less likely to find that discovery of the P2P source code is material to the full array of charges.

## B. Litigating Defense Motions

Regardless of the comprehensiveness of the government's voluntary disclosures, some defendants faced with few viable defenses to charges grounded in an undercover P2P download and subsequent search warrant will move to compel disclosure of a P2P tool's source code. The government should in all cases object to these requests on both materiality and law enforcement privilege grounds.

FED. R. CRIM. P. 16 requires the government to disclose, upon the defendant's request, all “documents . . . within the government's possession, custody, or control . . . [that are] *material* to

---

<sup>43</sup> See, e.g., *United States v. Case*, No. 13cr120, Decision and Order Denying Motion to Suppress (E.D. Wisc. Mar. 17, 2014) at 6-7 (denying motion to suppress grounded in defendant's unsupported claim that RoundUp was invasive).

preparing the defense.”<sup>44</sup> In order to compel disclosure “[a] defendant must make a threshold showing of materiality.”<sup>45</sup> In doing so, “[n]either a general description of the information sought nor conclusory allegations of materiality suffice; a defendant must present facts which would tend to show that the Government is in possession of information helpful to the defense.”<sup>46</sup> Accordingly, it is defendant’s burden to proffer, with factual support, which potential defense could be supported by specific exculpatory information theoretically contained in the requested materials.<sup>47</sup>

When faced with such motions, in addition to objecting on Rule 16 grounds, the government should always assert the law enforcement privilege early in the litigation. Even if a district court rules in favor of the government on materiality grounds, the government should be certain to create a careful record supporting invocation of the privilege in the event that an appellate court disagrees with the trial court’s Rule 16 analysis. The law enforcement privilege protects sensitive investigative techniques, such as the type and precise location of equipment used in electronic surveillance;<sup>48</sup> information concerning the location of posts used by surveillance agents;<sup>49</sup> an agency’s investigatory files or information regarding those files;<sup>50</sup> reports made by undercover agents;<sup>51</sup> and other aspects of law enforcement operations. The purpose of the privilege “is to prevent disclosure of law enforcement techniques and procedures, to preserve the confidentiality of sources, to protect witness and law enforcement personnel, to safeguard the privacy of individuals involved in an investigation, and otherwise to prevent interference with an investigation.”<sup>52</sup> “Just as the disclosure of an informer’s identity may destroy his future usefulness in criminal investigations, the identification of a hidden observation post will likely destroy the future value of that location for police surveillance.”<sup>53</sup>

When asserting the law enforcement privilege, the government should suggest that the district court adopt the *Pirosko* balancing test, weighing the government’s investigative concerns against the needs articulated by the defendant.<sup>54</sup> The government should emphasize the need for a defendant to make some showing of government “wrongdoing” to overcome the privilege.<sup>55</sup> To make a convincing case of government need, prosecutors should clearly articulate the harm threatened by disclosure of sensitive materials, e.g., producing either the source code or an executable version of proprietary software to a defendant. First and foremost, the disclosure of source code will enable defendants to access law enforcement’s database of hash values of known child pornography images. In other words, the defense team will be able to ascertain the full universe of images previously identified as child pornography by law enforcement agents using the tool in question. This would have the same impact, essentially, as disclosing a hidden observation post: if offenders are able to identify the specific child pornography files

---

<sup>44</sup> FED. R. CRIM. P. 16(a)(1)(E)(i) (emphasis supplied).

<sup>45</sup> *United States v. Santiago*, 46 F.3d 885, 894 (9th Cir. 1995); *see also* *United States v. Ross*, 511 F.2d 757, 762 (5th Cir. 1975) (defendant must demonstrate that the sought after information bears more than some “abstract logical relationship to the issues in the case”).

<sup>46</sup> *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990); *see also* *United States v. Carrasquillo-Plaza*, 873 F.2d 10, 12-13 (1st Cir. 1989).

<sup>47</sup> *See, e.g.,* *Pirosko*, 787 F.3d at 367-69; Feldman, 2015 WL 248006 at 6-7.

<sup>48</sup> *See* *United States v. Van Horn*, 789 F.2d 1492, 1507-08 (11th Cir. 1986) and *United States v. Cintolo*, 818 F.2d 980, 1002 (1st Cir. 1987).

<sup>49</sup> *See* *United States v. Harley*, 682 F.2d 1018, 1020-21 (D.C. Cir. 1982) and *United States v. Green*, 670 F.2d 1148, 1155 (D.C. Cir. 1981).

<sup>50</sup> *See* *Raz v. Mueller*, 389 F. Supp. 2d 1057, 1061-62 (W.D. Ark. 2005).

<sup>51</sup> *See* *In re The City of New York*, 607 F.3d 923, 928-29 (2d Cir. 2010).

<sup>52</sup> *In re Dep’t of Investigation of City of New York*, 856 F.2d 481, 484 (2d Cir. 1988); *see* *Commonwealth of Puerto Rico v. United States*, 490 F.3d 50, 64 (1st Cir. 2007).

<sup>53</sup> *Green*, 670 F.2d at 1155; *Cintolo*, 818 F.2d at 1002 no.13 (holding the privilege protects secret surveillance information).

<sup>54</sup> *Pirosko*, 787 F.3d at 367.

<sup>55</sup> *Id.* at 366.

law enforcement tools are seeking out, offenders could simply trade other child pornography files, or alter a single pixel in files contained in the law enforcement database so that those files generate an entirely different hash value.<sup>56</sup> Disclosure of the hash value database is problematic for a second reason: it would provide offenders with a road map for how to more efficiently obtain the listed child pornography files, because each hash value specifically identifies a particular child pornography file shared on P2P networks. If even a single offender was able to obtain this database, there is no doubt that it would become an immensely valuable commodity for the greater offender community, and be rapidly shared among that group. After all, what could be more valuable to those who seek out child pornography than a list enabling acquisition of millions of child pornography files? Finally, disclosure of a proprietary P2P tool's source code would disclose the covert identity used by law enforcement in the public portions of the pertinent P2P network. If offenders become aware of the identity used by law enforcement while downloading child pornography, those offenders could work to avoid detection, undermining the effectiveness of the tools employed by those investigators.

In all cases, prosecutors should consult with experts closely familiar with the particular law enforcement tool at issue because each tool's source code and user's manual may contain additional, tool-specific information that warrants protection.

### **C. Options for When Disclosure is Ordered**

If a district court disagrees with the substantial precedent rejecting defense requests for disclosure of proprietary P2P source code and instead mandates production, several options are available to the government. First, the government can potentially appeal any such ruling on an interlocutory basis. Of course, this is an unusual step and requires approval at various levels. In the event that an appeal of an adverse ruling is not possible, prosecutors should consult with appropriate investigative agencies to chart a course of action. Under no circumstances should prosecutors produce source code or an executable version of P2P software without first consulting with supervisory personnel at the investigative agency with custody of the intellectual property at issue. If there is no way to satisfy a court's order without disclosing information that will threaten the viability of future investigations, in many cases the government will be in a position (depending on whether remaining evidence is sufficient to establish all elements of certain charged offenses) to forego use at trial of any evidence directly obtained through a law enforcement tool. Adopting this approach would require the defendant to make an extraordinarily difficult prima facie showing that production of the source code could in some way support an affirmative defense to charged conduct outside the scope of the undercover session. Accordingly, in response to mandated disclosure of proprietary source code, the government may choose to supersede an indictment (or dismiss certain counts) so as to focus the prosecution exclusively on evidence derived from the forensic review of defendant's electronic storage materials, as well as other evidence of guilt such as a confession, rather than on undercover P2P downloads.

## **IV. Conclusion**

As law enforcement online investigative tools advance and expand beyond P2P child pornography investigations, the importance of protecting those tools will only increase. Answering defense requests for P2P tool source code by providing comprehensive information, supported by expert testimony explaining the functionality of and pertinent discoverable data obtained from the law enforcement tool at issue, should generally be sufficient to demonstrate that FED. R. CRIM. P. 16 does not require disclosure of the tool's source code. However, even where a defendant convinces a court that a

---

<sup>56</sup> *Cf. e.g., Van Horn*, 789 F.2d at 1507 (“the identification of a hidden observation post will likely destroy the future value of that location for police surveillance”).

tool's source code is material to his defense, prosecutors can point to the growing body of case law recognizing that the law enforcement privilege trumps the defendant's need for disclosure.

## ABOUT THE AUTHORS

□ **Jeffrey H. Zeeman** is a Trial Attorney at DOJ's Office of Enforcement Operation's Policy and Statutory Enforcement Unit. Jeff has worked at the Department since 2008, including eight years at DOJ's Child Exploitation and Obscenity Section as a Trial Attorney and as Acting Assistant Deputy Chief for Policy and Legislation. Jeff has trained federal, state, and local investigators at the National Advocacy Center and the National Crimes Against Children Conference. Jeff previously authored "Criminal Conduct of Victims: Policy Considerations" in the November 2017 edition of the United States Attorneys' Bulletin and "Meeting the Government's Discovery Obligations in Child Exploitation Cases" in the September 2011 edition of the United States Attorneys' Bulletin.

□ **Joanne C. Pasquarelli** is an Assistant General Counsel at the FBI's Office of the General Counsel. Joanne began her work for the FBI in 1989 as an engineer and then moved to the General Counsel's office in 1998. Joanne's work has focused on providing legal guidance to technically complex criminal investigations, primarily online investigations. Joanne regularly taught the legal component for the FBI's On-line Covert Employee certification course from 2006 until 2015. She authored Appendix L to the FBI's Domestic Investigations and Operations Guidelines which provides policy guidelines for online investigations. In Joanne's role as counsel to the FBI's Violent Crimes Against Children Section, she often assists prosecutors in their efforts to protect law enforcement's interests in the wake of defense's broad discovery requests.

Page Intentionally Left Blank

# Transnational Drug Trafficking Act of 2015

*Stephen Sola*  
*Acting Assistant Deputy Chief*  
*Narcotic and Dangerous Drug Section*  
*Criminal Division*  
*United States Department of Justice*

*Paul Laymon*  
*Senior Litigation Counsel*  
*Narcotic and Dangerous Drug Section*  
*Criminal Division*  
*United States Department of Justice*

*Thomas Johnson*  
*Trial Attorney*  
*Narcotic and Dangerous Drug Section*  
*Criminal Division*  
*United States Department of Justice*

## I. Introduction

On May 16, 2016, Congress enacted the Transnational Drug Trafficking Act of 2015 and strengthened the government’s ability to prosecute foreign drug traffickers pursuant to 21 U.S.C. § 959 (2016).<sup>1</sup> Section 959, one of the most important tools to prosecute international narcotics traffickers, criminalizes extraterritorial manufacturing or distribution of certain controlled or dangerous substances. Before the 2016 amendment, prosecutors bringing § 959 cases often found mens rea to be their most significant challenge. The statute required that the foreign drug trafficker defendant intended or had knowledge that the drugs at issue were destined for the United States. Or, in other words, that the international drug trafficker intended or knew that the transactions at issue had a United States nexus.

Congress’s recent amendment to § 959(a) revised the nexus requirement by broadening § 959(a)’s mens rea component beyond intent or actual knowledge. Borrowing from other criminal statutes such as 21 U.S.C. § 841(c)(2),<sup>2</sup> which criminalizes the domestic distribution of chemical precursors for use in manufacturing or distributing drugs such as methamphetamine, Congress extended the reach of § 959 to include the manufacture or distribution of a Schedule I or II controlled substance, or a listed chemical “intending, knowing, *or having reasonable cause to believe*” that such substance or

---

<sup>1</sup> 21 U.S.C. § 959 (2016).

<sup>2</sup> 21 U.S.C. § 841(c)(2).

chemical will be unlawfully imported into the United States (*italics indicate the change in the law*).<sup>3</sup>

Congress also added § 959(b), which applies the “reasonable cause to believe” standard to the international manufacture and distribution of precursor chemicals. This legislative addition addresses situations where precursor chemicals such as pseudoephedrine (a methamphetamine precursor chemical) are distributed internationally, for instance from China to Mexico, for the purpose of manufacturing a controlled substance (methamphetamine), and then the controlled substance (methamphetamine) is illegally imported from Mexico into the United States.

A recent case brought by the Narcotic and Dangerous Drug Section’s litigation unit illustrates § 959’s mens rea component prior to Congress’s 2016 amendment. In *United States v. Borda*,<sup>4</sup> the government presented evidence that Defendants Christian Borda and Alvaro Alvaran-Velez conspired to distribute thousand-kilo loads of cocaine over the course of three separate 2005 transactions. In the first of these transactions, the Defendants arranged for the transportation of approximately 1,553 kilograms of cocaine hidden in drums of palm oil from Cartagena, Colombia, to Puerto Progreso, Mexico.<sup>5</sup> This cocaine was ultimately transported into the United States.<sup>6</sup> At trial, the Defendants did not meaningfully contest that they conspired to smuggle cocaine between Colombia and Mexico.<sup>7</sup> Rather, the Defendants argued that they lacked knowledge that the cocaine was destined for the United States after arrival in Mexico.<sup>8</sup> Although the government was ultimately successful in proving that the Defendants were aware that the drugs were destined for the United States, the trial counterintuitively turned on the existence of a United States nexus—and not on the Defendants’ conceded efforts to smuggle thousands of kilograms of cocaine between Central and South America.<sup>9</sup>

Congress’s recent amendment to § 959 undoubtedly strengthens the government’s case against drug traffickers like *Borda*, but how heavily can prosecutors rely on the new “reasonable cause to believe” standard when a case is on the margins? With the preceding in mind, this article analyzes the new boundaries of § 959 by exploring analogous case law and the legislative history of the Act. Circuit courts interpreting similar statutes are split on various aspects of the “reasonable cause to believe” mens rea standard, including whether the standard is subjective or objective. Courts facing these issues under § 959 should look to the legislative history of the Act, especially its purpose. Although the Committee Report does not precisely define “reasonable cause to believe,” the legislative history underscores Congress’s intent to target international narcotics traffickers who attempt to isolate themselves from information concerning the destination of their products.

By enacting this legislation into law, Congress clearly intended to facilitate United States drug prosecutions of foreign narcotics traffickers. The purpose of this article is to encourage prosecutors to bring more cases pursuant to § 959, thereby reducing the supply of illicit narcotics in the United States. The article includes five sections. Following this introduction, Part II discusses the legislative history of the Act. Part III reviews analogous statutes and accompanying case law. Part IV returns to *United States v. Borda*, applying the “reasonable cause to believe” standard to the facts of a recent § 959(a) trial

---

<sup>3</sup> The term “listed chemical” is a defined term under the Controlled Substances Act. “Listed chemicals” are divided into two categories: List I and List II. 21 U.S.C. § 802(33) (defining “listed chemicals”). List I chemicals are “used in manufacturing a controlled substance in violation of [the Controlled Substances Act]” and are “important to the manufacture of the controlled substances.” 21 U.S.C. § 802(34). List II chemicals are chemicals (other than List I chemicals) that are “used in the manufacturing a controlled substance in violation of [the Controlled Substance Act].” 21 U.S.C. § 802(35).

<sup>4</sup> *United States v. Borda*, 848 F.3d 1044, 1051 (D.C. Cir. 2017) (D.C. Cir.), cert. denied, 137 S. Ct. 2315 (2017).

<sup>5</sup> *Id.* at 1052.

<sup>6</sup> *Id.* at 1054.

<sup>7</sup> *Id.* at 1053.

<sup>8</sup> *Id.*

<sup>9</sup> *Id.*

prosecuted by the Narcotic and Dangerous Drug Section. Part V is the conclusion, and urges prosecutors to renew their efforts to investigate and prosecute extraterritorial drug traffickers under the newly amended § 959.<sup>10</sup>

## II. Legislative History

On May 16, 2016, the Transnational Drug Trafficking Act of 2015, Senate Bill 43 (S.32), was signed into law. S.32, 114th Cong. (2nd Sess. 2015). On May 10, 2016, the bill passed on a voice vote in the U.S. House of Representatives, and on October 7, 2015, the U.S. Senate passed the bill by unanimous consent.<sup>11</sup>

The substantive legislative history for the Act consists largely of the remarks of Senator Feinstein—who was the principal Senate sponsor—the House Judiciary Committee Report, and the House floor debate. There is scant legislative background from the Senate’s consideration of the bill.<sup>12</sup> On January 6, 2015, S.32 was introduced, and on September 17, 2015, the Senate Judiciary Committee approved the legislation without amendment and without a written Committee Report. On October 7, 2015, the full Senate took up the measure and passed it without amendment after remarks by Senator Feinstein.<sup>13</sup>

In contrast, the House of Representatives published a House Judiciary Committee Report (Committee Report or Report) and held a floor debate. On July 29, 2015, House Bill 3380, the companion bill to S.32, was introduced. On April 20, 2016, the House Judiciary Committee approved the bill without amendment,<sup>14</sup> and on May 10, 2016, the House of Representatives debated the legislation and then passed it on the suspension calendar without a recorded vote.<sup>15</sup> The bill was then sent to the President and signed into law on May 16, 2016. As such, Senator Feinstein’s statements, the House Judiciary Committee Report, and the House floor debate represent the most comprehensive explanation of Congressional intent.

### A. Senator Feinstein’s Remarks

Upon introducing the measure, Senator Feinstein stated that the legislation was designed to provide the Department of Justice “with crucial tools to combat the international drug trade.”<sup>16</sup> Senator Feinstein noted that the legislation “put in place penalties for extraterritorial drug traffickers when individuals have *reasonable cause to believe* that illegal drugs will be trafficked into the United States,” while current law required that drug traffickers must “know that illegal drugs will be trafficked into the

---

<sup>10</sup> *Id.*

<sup>11</sup> Library of Congress Legislative Tracking, S.32-Transnational Drug Trafficking Act of 2015, <https://www.congress.gov/bill/114th-congress/senate-bill/32/actions> (last visited Sept. 27, 2017).

<sup>12</sup> The absence of legislative history in the Senate is most likely attributable to the fact that the Senate had passed the legislation in previous Congressional sessions, only to have the House of Representatives fail to consider the measure. *See* S.32, 161, CONG. REC. 18, (daily ed. Jan. 6, 2015) (statement of Sen. Feinstein) (stating that the legislation “passed the Senate unanimously in the last Congress”); S.706, 159, Cong. Rec. 2590-91, (daily ed. Apr. 11, 2013) (statement of Sen. Feinstein) (stating again that the Transnational Drug Trafficking Act “passed the Senate unanimously in the last Congress”).

<sup>13</sup> Library of Congress Legislative Tracking, S. 32-Transnational Drug Trafficking Act of 2015 <https://www.congress.gov/bill/114th-congress/senate-bill/32/actions> (last visited Sept. 27, 2017).

<sup>14</sup> H.R. REP. NO. 114-603, at 2 (2015).

<sup>15</sup> 162 CONG. REC. H2175-01.

<sup>16</sup> S. 32, 161, CONG. REC. 18 (daily ed. Jan. 6, 2015) (statement of Sen. Feinstein).

United States.”<sup>17</sup> Thus, the legislation “would lower the knowledge threshold to reasonable cause to believe.”<sup>18</sup>

As Senator Feinstein explained, the Justice Department informed Congress that drug traffickers from source countries such as Colombia, Bolivia, and Peru manufactured cocaine and then sold it to Mexican cartels, who, in turn, illegally imported the drugs into the United States. Senator Feinstein expressed concern that the ability of the United States to prosecute those traffickers was limited because there is “often no direct evidence of their knowledge that illegal drugs were intended for the United States.”<sup>19</sup>

## B. House Judiciary Committee Report

The legislative history from the House of Representatives is consistent with the intent of the bill as expressed by Senator Feinstein. As the House Judiciary Committee Report stated, Congress advanced the legislation in response to input from federal law enforcement, which noticed an evolution in international drug trafficking patterns for South and Central American cartels. As the Report found:

Increasingly, these organizations [South and Central American drug trafficking organizations] no longer rely on distribution networks in the United States, but instead sell their illicit products to Mexican traffickers, who in turn, import the narcotics into the United States. Under current law, Federal prosecutors must prove that these ‘source-nation’ manufacturers, whole distributors, brokers and transporters, intend for the drugs to reach the United States.<sup>20</sup> But the use of intermediary traffickers in Mexico makes it difficult, if not impossible in some instances, for the Government to prove knowledge that the drugs are bound for America. The result is that ‘source-nation’ traffickers escape prosecution because they claim ignorance of the drugs’ ultimate destination.<sup>21</sup>

The legislation addresses the willful blindness of source-country drug traffickers by revising the mens rea threshold from “knowing” or “intending” to a “reasonable cause to believe” that the Schedule I or II controlled substances will be illegally imported into the United States.<sup>22</sup> As a result, “under this standard, a federal prosecutor could use the circumstantial evidence of the drugs’ nexus to the United States (*use of U.S. dollars, drug route, packaging, etc*) as *direct evidence* that the defendant had reasonable cause to believe that the drugs were destined for the United States.”<sup>23</sup>

---

<sup>17</sup> *Id.* (emphasis added).

<sup>18</sup> *Id.*

<sup>19</sup> *Id.*; With regard to precursor chemicals, Senator Feinstein somewhat oversimplified what the proposed legislation would accomplish. She noted that the legislation addressed “precursor chemical producers from foreign countries, such as pseudoephedrine used for methamphetamine, who illegally ship precursor chemicals into the United States knowing that these chemicals will be used to make illegal drugs.” S. 32, 161, CONG. REC. 19 (daily ed. Jan. 6, 2015) (statement of Sen. Feinstein). In fact, the legislation is slightly more nuanced. It prohibits the extraterritorial manufacture or distribution of listed chemicals knowing, intending or having reasonable cause to believe that they will be unlawfully imported into the United States. In addition, it prohibits the extraterritorial manufacture or distribution of a listed chemical knowing or intending it will be used to manufacture a controlled substance, and intending, knowing or having reasonable cause to believe that the controlled substance will be unlawfully imported into the United States.

<sup>20</sup> Note: the House Report also should have stated that the law in effect at the time prohibited the manufacture or distribution when the offender “knows” that the narcotics will be illegally imported into the United States. *See* 21 U.S.C. § 959(a) (2015).

<sup>21</sup> H.R. REP. NO. 114-603, at 2 (2015).

<sup>22</sup> *Id.* The House Report stated: “This amendment will allow the Government to argue that the defendant had ‘reasonable cause to believe’ the drugs he was conspiring to traffic were bound for the United States.”

<sup>23</sup> *Id.* (emphasis added).

The Committee also stated that the legislation filled a gap in the Controlled Substance Import Export Act, 21 U.S.C. § 951, et seq. (CSIEA), regarding international precursor chemical trafficking. Previously, the law only prohibited the manufacture or distribution of a listed chemical intending or knowing that such chemical would be unlawfully imported into the United States.<sup>24</sup> In the Report's section-by-section analysis, the Committee stated that the bill "amends the CSIEA to prohibit extraterritorial trafficking of listed chemicals for the manufacture of controlled substance that are to be unlawfully imported into the United States, and similarly contains a 'reasonable cause to believe' standard."<sup>25</sup>

### C. House Floor Debate

On May 10, 2016, the House of Representatives debated the measure.<sup>26</sup> Judiciary Committee Chairman Goodlatte told members of the House that the bill was necessary because "international drug traffickers know that if they simply employ a middleman to take the drugs . . . and transport them into the United States, it makes it much harder, if not impossible, for U.S. law enforcement to prosecute them."<sup>27</sup> Chairman Goodlatte further explained:

[U]nder current law, the Government must prove that a trafficker knew the drugs were headed for the United States. Drug trafficking organizations in Colombia, Peru, Ecuador, and other Central and South American source nations sell their illicit products to Mexican traffickers who, in turn, traffic the drugs into the United States.

This makes it difficult, under current law, for Federal prosecutors to make cases against such source nation manufacturers, wholesale distributors, brokers and transporters since direct evidence of their intent that the drugs are bound for the United States is difficult, if not impossible, to develop.

The result is that source nation malefactors who produce and distribute illegal narcotics escape prosecution under U.S. law because they feign ignorance of the drug's ultimate destination. This has happened with increasing regularity over the past several years.

. . .

---

<sup>24</sup> The House Report stated:

Current law only addresses extraterritorial trafficking of listed chemicals that results in the smuggling of the listed chemicals themselves or the finished controlled substances into the United States. H.R. 3880 would amend the CSIEA to reach chemical traffickers who knowingly facilitate and benefit from the trafficking operation, even if they do not actually take part in the manufacturing and trafficking conspiracy.

H.R. REP. NO. 114-603, at 2 (2015).

This explanation requires some interpretation. Current law in effect prior to the passage of the instant legislation did in fact prohibit the illegal distribution of listed chemicals that result in the illegal importation of the listed chemical into the United States, and current law did prohibit the illegal importation of the finished controlled substances themselves, but current law in effect prior to the passage of the legislation *did not* prohibit the trafficking of the listed chemicals that resulted in the smuggling of the finished controlled substances into the United States. The entire purpose of H.R. 3380 with regard to listed chemicals was to render such conduct illegal, so current law prior to the passage of S.32/H.R. 3380, did not prohibit the extraterritorial distribution of listed chemicals that were manufactured into controlled substances and that were subsequently illegally smuggled into the United States.

<sup>25</sup> *Id.*

<sup>26</sup> Because the bill text of the House and Senate versions were identical and the Senate had already passed its version, the House debated and then subsequently passed the Senate bill, which avoided the need to conference the legislation between the House and Senate. *See* 162 Cong. Rec. 2175 (daily ed. May 10, 2016) (statement of Rep. Goodlatte making a motion to suspend the House rules and seeking passage of S.32 and stating that "S.32, the Transnational Drug Trafficking Act of 2015, is identical to H.R. 3380").

<sup>27</sup> 162 CONG. REC. H2175-01 (daily ed. May 10, 2016) (statement of Rep. Goodlatte).

This amendment will permit Federal prosecutors to pursue extraterritorial drug traffickers who are not directly smuggling drugs into the United States but who facilitate it.<sup>28</sup>

Echoing the Judiciary Committee Chairman's comments, Rep. Tom Marino, one of the bill's primary sponsors, stated that the bill targeted "leaders of sophisticated, often multi-national drug-trafficking organizations with expansive networks of distribution internationally."<sup>29</sup> Rep. Marino noted that "in many instances, the final destination" of the narcotics is the United States, but "these individuals can hide their knowledge or insert additional middlemen to potentially evade prosecution."<sup>30</sup>

Following the close of debate, the House of Representatives passed S.32, and the bill was then sent to the President and signed into law on May 16, 2016, without further comment.

### III. Case Law

Over one year after the effective date of the Transnational Drug Trafficking Act of 2015, there is no substantive case law regarding the amendments to § 959. Two circuit courts noted the amendments,<sup>31</sup> but neither analyzed the new § 959 mens rea of "reasonable cause to believe." As such, interpretations of § 959 that go beyond legislative history must look to analogous case law to analyze the framework of the amended statute. The long history of "reasonable cause to believe" as a mens rea standard suggests that § 959 is constitutionally sound. However, courts disagree as to whether statutes similar to § 959 call for an objective or subjective understanding of "reasonable cause to believe." This circuit split meaningfully affects the government's burden.

#### A. Criminal Statutes Containing a "Reasonable Cause to Believe" Mens Rea

The breadth of the newly amended § 959 will primarily turn on how courts interpret the mens rea of § 959(a) and (b). Congress has passed at least one dozen criminal statutes<sup>32</sup> with a "reasonable cause to

---

<sup>28</sup> *Id.*

<sup>29</sup> 162 CONG. REC. H2175-01 (daily ed. May 10, 2016) (statement of Rep. Marino).

<sup>30</sup> 162 CONG. REC. H2178.; Similarly, Rep. Sheila Jackson Lee, during her floor statement, commented that "[s]ome drug traffickers are aware of the methods used to charge and then extradite foreign criminals into the U.S. for prosecution," and "drug traffickers simply avoid any discussion of the destination of the drug shipments" in order to circumvent the mens rea element of the offense. *See* H.R. 3380, 162, Cong. Rec. 2176 (daily ed. May 10, 2016) (statement of Rep. Jackson Lee).

<sup>31</sup> *United States v. Epskamp*, 832 F.3d 154, 170 n.6 (2d Cir. 2016); *United States v. Thelmaque*, 2017 WL 2645540, at 5 (11th Cir. June 20, 2017) (unpub.).

<sup>32</sup> *See* 18 U.S.C. § 793(a) (2016) (obtaining information concerning national defense with "intent or reason to believe that the information is to be used to the injury of the United States"); 18 U.S.C. § 842(h) (2016) (possessing, transporting, or selling explosive materials "knowing or having reasonable cause to believe" that the explosive materials were stolen); 18 U.S.C. § 922(d) (2016) (selling or otherwise disposing of any firearm or ammunition to any person "knowing or having reasonable cause to believe" that such person meets one of nine criteria); 18 U.S.C. § 231(a)(1) (2016) (teaching or demonstrating to another the use, application, or making of any firearm or explosive "knowing or having reason to know" that it will be unlawfully employed); 18 U.S.C. § 231(a)(2) (2016) (transporting the firearm or explosive described in § 231(a)(1); 18 U.S.C. § 1384 (2016) (keeping a house of prostitution, near a military or navy establishment, "knowing or with good reason to know" that it is intended to be used for prohibited purposes); 18 U.S.C. § 1521 (filing false lien against federal judge or federal law enforcement officer in retaliation, "having reason to know" such lien is false); 18 U.S.C. § 1546(b) (2016) (using an identification document "knowing (or having reason to know)" that the document was not issued lawfully or is false); 18 U.S.C. § 2251(a)(6) (2016) (using a minor with intent that such minor engage in sexually explicit conduct, for the purpose of procuring any visual depiction of such conduct, if such person "knows or has reason to know" that such visual depiction will be transported in interstate commerce); 18 U.S.C. § 2512(1) (2016) (manufacturing or distributing devices for the surreptitious interception of communications "knowing or having reason to know" that the design of the device renders it useful for surreptitious interceptions); 21 U.S.C. § 843(a)(6) (2016) (possessing equipment, chemicals, products, or materials which may be used to manufacture a controlled substance or listed chemical,

believe” or substantially similar mens rea since 1917.<sup>33</sup> Prosecutors may rely on these as references to bolster their understanding of the new mens rea in § 959.

Perhaps the statute most like the amended § 959 is 21 U.S.C. § 841(c)(2).<sup>34</sup> Section 841(c)(2) prohibits possession or distribution of a listed chemical, knowing or having reasonable cause to believe, that the listed chemical will be used to manufacture a controlled substance. Section 841(c)(2) has withstood constitutional challenges for vagueness, and the statute’s “reasonable cause to believe” scienter has been deemed to be constitutionally sufficient.<sup>35</sup> So prosecutors may cautiously presume that the newly amended § 959 will also survive constitutional challenges.

## **B. The Objective or Subjective Nature of the “Reasonable Cause to Believe”**

A wealth of case law exists concerning the numerous statutes containing mens rea analogous to § 959. Although new issues may arise specific to § 959, prosecutors should be aware that one major circuit split already exists regarding the interpretation of a “reasonable cause to believe” mens rea in § 841(c)(2). Courts disagree as to whether this mens rea requires an objective perspective, a subjective perspective, or a combination of the two. That is, as these circuit courts have framed the issue, the key inquiry is: does “reasonable cause to believe” mean (1) the fact finder must first determine what facts the defendant knew and then determine whether a reasonable person knowing those facts would have a “reasonable cause to believe,” an approach which is both subjective and objective; or does it mean (2) the fact finder must first determine what facts the defendant knew and then determine whether that particular defendant would have a “reasonable cause to believe,” which is a more subjective approach.

The majority view, adopted by the Eighth, Ninth, and Eleventh Circuits, is that the fact finder must first determine what facts the defendant knew and then determine whether a reasonable person knowing those facts would have a “reasonable cause to believe.”<sup>36</sup>

---

“knowing, intending, or having reasonable cause to believe” it will be used to manufacture a controlled substance or listed chemical); 21 U.S.C. § 960(d)(3) (2016) (importing or exporting listed chemicals “knowing or having reasonable cause to believe” that the chemicals will be used to manufacture a controlled substance).

<sup>33</sup> See 18 U.S.C. § 793 (2016) (succeeding the Espionage Act of 1917).

<sup>34</sup> 21 U.S.C. § 841(c)(2).

<sup>35</sup> See, e.g., *United States v. Jae Gab Kim*, 449 F.3d 933, 941-43 (9th Cir. 2006) (holding that a “reasonable cause to believe” scienter is sufficiently clear to meet vagueness requirements); *United States v. Biro*, 143 F.3d 1421, 1429-30 (11th Cir. 1998) (analyzing 18 U.S.C. § 2512(1)); *United States v. Featherston*, 461 F.2d 1119, 1121 (5th Cir. 1972) (discussing 18 U.S.C. § 231(a)). Section 841(c)(2), and the numerous other statutes containing similar mens rea components, confirm the longstanding and widespread acceptance in United States criminal law of a “reasonable cause to believe” mens rea. See, e.g., *United States v. Gorin*, 312 U.S. 19 (1941) (interpreting a “reasonable cause to believe” mens rea standard in its analysis of the constitutionality of the Espionage Act of 1917); see also *United States v. Saffo*, 227 F.3d 1260, 1268 (10th Cir. 2000) (partial list of federal statutes containing “reasonable cause to believe” mens rea).

<sup>36</sup> See Jonathan L. Hood, *What is Reasonable Cause to Believe?: The Mens Rea Required for Conviction Under 21 U.S.C. § 841*, 30 PACE L. REV. 1360, 1361 (2010). See also *United States v. Galvan*, 407 F.3d 954, 957 (8th Cir. 2005) (rejecting defendant’s request for jury instruction that “reasonable cause to believe” required an inquiry into what he, the defendant, believed); *United States v. Kaur*, 382 F.3d 1155, 1157-58 (9th Cir. 2004) (approving district court instruction that “reasonable cause to believe” meant what a reasonable person would believe knowing what the defendant knew); *United States v. Johal*, 428 F.3d 823, 827-28 (9th Cir. 2005) (holding that the “reasonable cause to believe” requires a defendant knew facts that would cause a reasonable person to believe); *United States v. Prather*, 205 F.3d 1265, 1270 (11th Cir. 2000) (approving a supplemental jury instruction which defined “reasonable cause to believe” as what “an abstract reasonable person would believe if that abstract reasonable knew what the defendant knew.”). But see *United States v. Munguia*, 704 F.3d 596, 603 (9th Cir. 2012) (in which the Ninth Circuit erroneously interpreted *Kaur* as holding that “reasonable cause to believe” requires determining scienter “through the eyes of the particular defendant on trial.”).

The minority view, so far prevailing only in the 10th Circuit, is that the fact finder must first determine what facts the defendant knew, and then determine whether that particular defendant would have a “reasonable cause to believe the fact at issue.”<sup>37</sup>

The Seventh Circuit has recognized the split in the circuits and has written comprehensively about the circuit split, but has avoided addressing the issue.<sup>38</sup> However, at least one district court in the Seventh Circuit has concluded that the majority view is the correct approach.<sup>39</sup> In *Gulley*, on defendant’s motion for new trial, the district court rejected Gulley’s claim that the court erred by not giving Gulley’s proposed jury instruction, which would have instructed the jury that “reasonable cause to believe” meant “that facts and circumstances actually known to the defendant caused [the defendant] to believe.”<sup>40</sup> The district court agreed with the majority view and reasoned that “to hold otherwise would render the “reasonable cause to believe” statutory language superfluous . . .”<sup>41</sup>

In addition to the § 841(c)(2) cases, which likely will guide how courts will interpret the amended § 959, other circuits have interpreted the “reason to know” mens rea in other federal statutes listed. Though these cases offer less guidance compared to the cases interpreting § 841(c)(2), that guidance is nonetheless significant. Title 18, United States Code, Section 1521, prohibits retaliating against a federal judge by filing a false lien “having reason to know” such lien is false. Curiously, the Tenth Circuit concluded in a § 1521 case that “the jury may convict the defendant if a reasonable person who possessed the information possessed by the defendant would have the requisite knowledge of falsity.”<sup>42</sup> And, 18 U.S.C. § 2511(1)(d)<sup>43</sup> prohibits using the contents of any wire, oral, or electronic communication “having reasonable cause to know” the information was intercepted illegally. In *United States v. Wuliger*,<sup>44</sup> the Sixth Circuit found error in the district court’s instruction equating “reasonable cause to know a particular fact” with “reasonable foreseeability of such fact.” In the context of a prosecution under § 2511(1)(d), the court concluded that reasonable foreseeability was “only a factor to be considered with other circumstantial evidence in determining whether one has reason to know a fact.”<sup>45</sup>

#### IV. A § 959 Case Study: *United States v. Borda*

Researching the legislative history of the Transnational Drug Trafficking Act of 2016 and reviewing analogous statutes are helpful preparation for prosecutors seeking to bring a § 959 case to trial. But a practical application to facts may also be useful. With this in mind, this article now analyzes how a “reasonable cause to believe” standard might affect the government’s burden at trial by reviewing a pre-amendment § 959 District of Columbia case, *United States v. Borda*.

---

<sup>37</sup> See *United States v. Truong*, 425 F.3d 1282, 1289 (10th Cir. 2005) (rejecting the argument that “reasonable cause to believe” in § 841(c)(2) included “proof that a reasonable person in the defendant’s circumstances should have known”); *United States v. Buonocore*, 416 F.3d 1124, 1133 (10th Cir. 2005) (approving instructions that the “inquiry is entirely subjective, the inquiry is not to be viewed from the perspective of a hypothetical reasonable person”); *United States v. Saffo*, 227 F.3d at 1269 (“[R]easonable cause to believe . . . involves a subjective inquiry that looks to whether the particular defendant . . . had reasonable cause to believe . . . This requires scienter to be evaluated through the lens of this particular defendant, rather than from the perspective of a hypothetical reasonable man.”) (citing *State v. Smith*, 22 N.J. 59, 64-65, 123 A.2d 369 (1956)).

<sup>38</sup> *United States v. Khattab*, 536 F.3d 765, 769 (7th Cir. 2008).

<sup>39</sup> *United States v. Gulley*, 2014 WL 2522831, at 2-3 (S.D. Ill. June 4, 2014) (unpub.).

<sup>40</sup> *Id.* at 2.

<sup>41</sup> *Id.*

<sup>42</sup> *United States v. Williamson*, 746 F.3d 987, 994 (10th Cir. 2014) (citations omitted).

<sup>43</sup> 18 U.S.C. § 2511(1)(d).

<sup>44</sup> *United States v. Wuliger*, 981 F.2d 1497, 1503-04 (6th Cir. 1992).

<sup>45</sup> *Id.* at 1504.

In 2005, Borda was a major Colombian drug trafficker who transported thousands of kilograms of cocaine from Colombia to Mexico.<sup>46</sup> Borda did not transport cocaine directly to the United States, and specifically refused to do so when asked. Borda also was interested in transporting cocaine to Europe and actively schemed to transport cocaine there, though, in 2005, it was not clear he had ever done so.<sup>47</sup>

Borda's trial focused on one load shipped to Mexico known as the palm oil load.<sup>48</sup> Borda agreed to sell more than 1,500 kilograms of cocaine to his Mexican partner, with the understanding that the Mexican partner would pay Borda for the cocaine immediately after the Mexican partner received the cocaine in Mexico City.<sup>49</sup> Borda opened a palm oil business in Colombia to export palm oil and cocaine to Mexico. He hid the 1,500 kilograms of cocaine in numerous fifty-gallon drums of palm oil, which he shipped commercially from a port on the north coast of Colombia to a port on the east coast of Mexico.<sup>50</sup> Borda never asked his Mexican partner to identify the ultimate destination of the cocaine, although the Mexican partner indicated that the cocaine would be transported from the port to Mexico City.<sup>51</sup> All parties to the agreement knew, however, that Mexico was a transit country for large shipments of cocaine, not a final destination. Borda's agreement with his Mexican partner was that Borda would be paid more than six million dollars for the cocaine, and that money would be paid to Borda's lieutenant in Mexico City, who, in turn, would send the money to Borda in Colombia.<sup>52</sup>

As the cocaine was being received in the Mexican port, Borda's Mexican partner asked Borda for permission to transport the cocaine from that port to the Mexican city of Monterrey, less than two hours south of the United States border.<sup>53</sup> Borda agreed to the request. Several weeks later, the Mexican partner began sending bulk United States currency to Borda's lieutenant in Mexico City.<sup>54</sup> Over the course of several months, the lieutenant received more than six million dollars in United States currency.<sup>55</sup>

If Borda were tried under the revised version of § 959(a), the government would have to prove that Borda (1) distributed cocaine, (2) intending, knowing, or having reasonable cause to believe that the cocaine would be unlawfully imported into the United States.<sup>56</sup> At the outset, the legislative history of the Transnational Drug Trafficking Act of 2015 suggests that the government should be more confident in its case following the statute's amendment. That is because Congress added the "reasonable cause to believe" mens rea component in order to broaden the scope of extraterritorial drug activities that fall within the reach of § 959. As stated by Senator Feinstein, the 2016 amendments to § 959 "lower the knowledge threshold to reasonable cause to believe."<sup>57</sup> And, as noted by Chairman Goodlatte, Congress was concerned that "source nation malefactors who produce and distribute illegal narcotics escape prosecution under U.S. law because they feign ignorance of the drug's ultimate destination."<sup>58</sup> This legislative history should weigh in the government's favor if a court presented with facts like those in *Borda* were evaluating proposed jury instructions or engaging in factfinding.

Turning to the circuit split, whether the "reasonable cause to believe" should be interpreted on an objective or subjective basis, it is doubtful that Borda's case would have been meaningfully affected by

---

<sup>46</sup> Borda, 848 F.d, at 1051.

<sup>47</sup> *Id.* at 1054.

<sup>48</sup> *Id.*

<sup>49</sup> *Id.* at 1052.

<sup>50</sup> *Id.*

<sup>51</sup> *Id.* at 1052-53.

<sup>52</sup> *Id.* at 1052.

<sup>53</sup> *Id.*

<sup>54</sup> *Id.*

<sup>55</sup> *Id.*

<sup>56</sup> Borda went to trial, and was ultimately convicted under the pre-amendment version of § 959(a).

<sup>57</sup> S. 32, 161, CONG. REC. 18 (daily ed. Jan. 6, 2015) (statement of Sen. Feinstein).

<sup>58</sup> 162 CONG. REC. H2175-01 (daily ed. May 10, 2016) (statement of Rep. Goodlatte).

how the court rules.<sup>59</sup> If the court followed the majority view, the government would contend that “reasonable cause to believe the cocaine would be unlawfully imported into the United States” turned on what a reasonable man would have believed knowing what Borda knew. So what really did Borda know? Borda knew in 2005 that 1500 kilograms of his cocaine, sold to his Mexican partner, were likely not going to remain in Mexico, as Mexico in 2005 was not generally understood to have a domestic cocaine market which could profitably keep 1500 kilograms of cocaine. Borda also knew that his Mexican partner, apparently, intended to take the cocaine to Mexico City, and Mexico City in 2005 was a hub from which cocaine could be transported to the United States or to Europe, or even to Japan. Borda also knew, as the cocaine arrived in the Mexican port, that the cocaine was not going initially to Mexico City as planned, but would go first to the city of Monterrey, an inland Mexican city considerably north of Mexico City and about two hours south of the United States border. Borda knew that several weeks after the cocaine arrived in Monterrey, Borda’s lieutenant in Mexico City began receiving millions of dollars of bulk United States currency, and that the entire \$6 million dollars was paid to Borda’s lieutenant over several months.

Would a reasonable man, knowing what Borda knew, have “reasonable cause to believe” that the cocaine would be unlawfully imported into the United States? In the *Borda* trial, no co-conspirator testified that he (the co-conspirator) believed the cocaine was headed to the United States, but the practical equivalent in the evidence was that 1,500 kilograms of cocaine were going to an inland Mexican city relatively close to the United States border, and such city was a transit point, not a final destination. Borda knew there was a delay of several weeks from the time the cocaine was received in Monterrey until his lieutenant began receiving millions of dollars in United States currency, suggesting that the delay was caused by waiting for the cocaine to be sold in the United States and for the drug proceeds to be collected for return to Mexico City. Cash payments were made in United States currency, not pesos or euros, further suggesting that the drugs were sold in the United States. Thus, a reasonable man who knew what Borda knew would have “reasonable cause to believe” the cocaine would be imported into the United States.<sup>60</sup>

Would the outcome be any different if Borda were tried in the Tenth Circuit, and the government had to show that Borda knew facts from which Borda—not a hypothetical reasonable man—would have “reasonable cause to believe” that the cocaine was to be imported into the United States? Borda had lived in the United States in the early 1990s and had been convicted in Florida of distributing cocaine. The subjective approach, as employed in the Tenth Circuit, would have permitted the government to argue that viewing what Borda knew, through the lens of a defendant quite familiar with drug trafficking in the United States, supported “reasonable cause to believe” the cocaine would be imported into the United States.<sup>61</sup>

Regardless of whether the *Borda* case were tried in a district that followed the objective or subjective approach, the “reasonable cause to believe” standard is a more favorable mens rea standard for the government than the “knowing” or “intending” standard under § 959. As a result, the passage of the

---

<sup>59</sup> The authors of the present article generally agree with the Southern District of Illinois’s finding in *Gulley* that the majority view is correct, and that “to hold otherwise would render ‘the reasonable cause to believe’ statutory language superfluous . . .” *United States v. Gulley*, 2014 WL 2522831, at 2 (S.D. Ill. June 4, 2014) (unpub.). However, prosecutors in circuits which have not definitively addressed the meaning of “reasonable cause to believe” should consult Criminal Appellate and NDDS for guidance.

<sup>60</sup> *Cf. United States v. Thelemaque*, 2017 WL 2645540, 3-4 (11th Circuit, June 20, 2017) (finding guilt under § 959 even though “no witness testified to hearing [defendant] say the words ‘I know the drugs are heading to the United States’”).

<sup>61</sup> However, a subjective interpretation of “reasonable cause to believe” may be a double-edged sword. *See United States v. Muessig*, 427 F.3d 856, 861-62 (10th Cir. 2005) (reviewing a § 959 case where the female defendant, a Vietnamese family grocery employee, claimed lack of knowledge and fostered blame for the scheme on her family patriarchs).

Transnational Drug Trafficking Act of 2015 is an improvement in terms of making it easier for the prosecution to demonstrate nexus.

## V. Conclusion

The Transnational Drug Trafficking Act of 2015 broadens the mens rea component of § 959 regarding the prosecution of international drug traffickers to include a “reasonable cause to believe” and criminalizes the extraterritorial manufacture and distribution of precursor chemicals. In addition to providing prosecutors with new tools to bring cases against foreign drug traffickers, the legislative history also includes implicit guidance. Congress expressed frustration with the efforts of international drug traffickers to carry on with impunity so long as they avoided hearing the words “United States” in their transactions. In this light, the Transnational Drug Trafficking Act of 2015 is both an effort to broaden § 959’s mens rea requirement as well as a signal that prosecutors should revisit opportunities to disrupt sophisticated and deliberate attempts to skirt United States law. Prosecutors should investigate the viability of international drug trafficking cases in the wake of the amendment to § 959, and prepare to reference case law concerning the “reasonable cause to believe” mens rea standard in other statutes.

### ABOUT THE AUTHORS

□ **Stephen Sola** is Acting Assistant Deputy Chief in the Litigation Unit of the Narcotic and Dangerous Drug Section, Criminal Division, United States Department of Justice. He has served as a Trial Attorney at NDDS for fourteen years, and previously worked in the DEA Office of Chief Counsel.

□ **Paul Laymon** is a Senior Litigation Counsel at the Narcotic and Dangerous Drug Section. He has served in the Department of Justice for twenty-three years. He also served as a Judge Advocate in the U.S. Army and as an Assistant District Attorney in Tennessee.

□ **Thomas Johnson** is a Trial Attorney at the Narcotic and Dangerous Drug Section. He joined the Criminal Division of the Department of Justice in 2016 through the Attorney General's Honors Program.

*NDDS wishes to thank Meaghan Baca, a second year law student at the University of New Mexico, for her invaluable assistance in conducting research and reviewing citations for the present article.*

Page Intentionally Left Blank

# Prosecuting Federal Hate Crimes

*Barbara Kay Bosserman*  
*Deputy Chief, Cold Case Unit*  
*Senior Legal Counsel*  
*Criminal Section*  
*Civil Rights Division*

*Angela M. Miller*  
*Attorney Advisor*  
*Criminal Section*  
*Civil Rights Division*

## I. Introduction

*On a June evening in Charleston, South Carolina, Bible study began at an African-American church that had played a significant role in both the historic and civic life of the black community since the early 1800s. As class began, the pastor noticed among the black congregants a young, white stranger and welcomed him to join the group in fellowship. Forty-five minutes later, as the group rose and bowed their heads in the final prayer, the stranger drew a semi-automatic and began to fire.*

*That stranger shot and killed the pastor and a second pastor who rushed to the pastor's aid. The other students in the Bible study scrambled to dive under tables in the fellowship hall. The gunman walked along the tables, shooting and killing the congregants. The gunman then calmly walked from the church to his car and drove away, leaving nine of the Bible study members dead or dying.*

*The gunman was arrested the next morning, with the murder weapon in the back seat of his car. He freely admitted what he had done, eagerly explaining to FBI interviewers that he had experienced a racial awakening after conducting online research at websites associated with white supremacist organizations. His research convinced him that whites needed to retake a position of dominance. He had decided to shoot black churchgoers to retaliate for what he perceived to be black-on-white crimes and to deliberately aggravate racial tensions to enhance the likelihood of a race war.*

*In December 2016, that gunman, Dylann Storm Roof, was convicted on all counts of a 33-count indictment, including 24 hate crime charges; he has been sentenced to death.<sup>1</sup>*

The Charleston shooting is a high-profile example of a federally prosecutable hate crime. A hate crime (sometimes called a bias-motivated crime) is a criminal offense motivated by some form of bias towards the victim or someone associated with the victim. The perpetrator's bias is what makes his act a "hate crime" as opposed to a simple murder, assault, or threat. Hate crimes are punished more severely than crimes with other kinds of motives because, in such attacks, victimization is not limited to the person who was directly hurt, killed, or threatened, but includes others who share the characteristics targeted by the perpetrator. In connection to the Charleston shooting, Roof expressed an intent to aggravate racial

---

<sup>1</sup> See Indictment at 1–13, *United States v. Roof*, 225 F. Supp. 3d 438 (D.S.C. 2016); see also Statement by Attorney General Loretta E. Lynch on the Sentencing of Dylann Roof, Office of Pub. Affairs, U.S. Dep't of Justice (Jan. 10, 2017).

tensions, perhaps even to start a race war. It is precisely this kind of terror and apprehension that hate crime laws seek to dispel.

This article focuses on federal hate crime statutes. Federal prosecutors should be aware, however, that most states have also enacted hate crime laws. These are far from uniform; different states have chosen to penalize different kinds of bias motivations and have structured their hate crime laws in different ways. The Anti-Defamation League has compiled a chart setting forth the different state laws.<sup>2</sup> Because not all hate crimes are prosecutable under federal law, federal prosecutors should familiarize themselves with state hate crime laws to be better positioned to refer appropriate cases to state authorities and to discuss with their state and local counterparts what venue is best suited to obtain the most just result.

In the federal system, there is no one hate crime law. In fact, there are four separate federal hate crime statutes, a civil rights conspiracy statute that may be used to prosecute hate crime conspiracies, a federal sentencing enhancement that can be used in conjunction with federal criminal prosecutions in which the defendant targets a victim based upon bias motivation, and general criminal statutes that are often used in the federal prosecution of hate crimes.

This article will attempt to provide an overview of each of these in turn.

## II. Federal Hate Crime Statutes

There are four specific federal hate crime statutes: 18 U.S.C. § 249 (The Hate Crime Prevention Act);<sup>3</sup> 42 U.S.C. § 3631 (Fair Housing);<sup>4</sup> 18 U.S.C. § 245(b)(2) (Federally Protected Activities);<sup>5</sup> and, 18 U.S.C. § 247 (Damage to Religious Property; Obstruction of Persons in the Free Exercise of Religious Beliefs).<sup>6</sup> Common to each is that the defendant's motive is an element of the offense; therefore, the government must prove the statutorily required bias motivation beyond a reasonable doubt at trial. Specifically, under the plain language of each hate crime statute, the government must prove that the defendant committed the act prohibited by the statute "because of" the characteristic at issue, be it race, color, religion, disability, or LGBT status.<sup>7</sup>

To prove the requisite motive, the government must prove that the bias motivation was a direct cause of the act. In other words, the government must prove that the assault or threat would not have happened but for the motivation.<sup>8</sup>

The exact type of animus that prosecutors must prove, as well as the underlying prohibited conduct, varies among the four federal hate crime statutes. To determine which statute is best suited for a particular offense, prosecutors should consider several questions, including whether the conduct involves an act of physical violence or just a threat of violence; what kind of bias motivation is at issue; and, whether there is evidence of any additional elements, such as interstate commerce, that are statutorily required for conviction.

---

<sup>2</sup> See ANTI-DEFAMATION LEAGUE, STATE HATE CRIME STATUTORY PROVISIONS (LAST UPDATED Fall 2017).

<sup>3</sup> 18 U.S.C. § 249 (2012).

<sup>4</sup> 42 U.S.C. § 3631 (2012).

<sup>5</sup> 18 U.S.C. § 245(b)(2) (2012).

<sup>6</sup> 18 U.S.C. § 247 (2012).

<sup>7</sup> See 18 U.S.C. §§ 247, 245(b)(2), 249 (2012); 42 U.S.C. § 3631 (2012).

<sup>8</sup> See *Burrage v. United States*, 134 S. Ct. 881, 881, 888 (2014) (holding that the phrase death "results from" a drug sale required "actual causality" and stressing that this usually "requires proof that the harm would not have occurred in the absence of—that is, but for—the defendant's conduct," and then comparing the term "but for" in the drug statute to the term "because of" in civil rights laws); see also *United States v. Miller*, 767 F.3d 585, 591-92 (6th Cir. 2014) (holding jury instruction that did not instruct on "but for" causality was improper in a federal hate crime case).

If a defendant willfully causes bodily injury or attempts to do so with a dangerous weapon, the most obvious statute implicated is 18 U.S.C. § 249, the Shepard-Byrd Hate Crime Prevention Act.<sup>9</sup> If the act of violence is motivated by racial bias (or bias against a religion or national origin that was deemed in 1865—the time of the passage of the Thirteenth Amendment—to be a race), the crime can be prosecuted under the “racial motivation” subsection of the statute and will not require proof of any additional element.<sup>10</sup> This subsection provides the most straightforward federal hate crime prosecution, as it requires a showing only of the physical assault itself and that the defendant acted because of the bias motivation. Similar offense conduct (willfully causing bodily injury or attempting to do so with a weapon), if based on a victim’s LGBT status, disability, gender, or based on religions or national origins not deemed racial at the time the Thirteenth Amendment was enacted is prosecutable under separate subsections of § 249 that additionally require the government to prove either that the offense was in or affecting interstate or foreign commerce,<sup>11</sup> or that it occurred in the Special Maritime or Territorial Jurisdiction (SMTJ) of the United States.<sup>12</sup>

Although § 249 is a tremendously useful tool for addressing hate crime violence involving physical assaults, it does not prohibit mere threats or vandalism. There are separate hate crime statutes, however, that do reach these types of conduct. There are federal statutes addressing hate crimes that interfere with housing rights (42 U.S.C. § 3631);<sup>13</sup> with federally-protected activities (18 U.S.C. § 245);<sup>14</sup> and that address vandalisms at houses of worship (18 U.S.C. § 247).<sup>15</sup> The statutes addressing hate crimes that interfere with housing or other protected rights cover crimes motivated by race, color, religion, or national origin; the criminal housing statute additionally covers crimes motivated by gender, disability, and family status. But because no federal hate crime law other than § 249 prohibits crimes based upon LGBT status, threats motivated by LGBT status can only be prosecuted in federal court if the conduct violates other general (non-hate crime) federal criminal statutes, such as laws prohibiting the delivery of threats by mail or the making of threats in interstate commerce. When a general criminal provision applies and the conduct was motivated by bias, however, the defendant’s sentence can be enhanced through the use of a hate crimes adjustment in the Sentencing Guidelines.

Three of the primary federal hate crime statutes require prosecutors to obtain appropriate DOJ certification before undertaking a prosecution.<sup>16</sup> Investigation, including grand jury investigation, may begin before a prosecutor obtains certification. What must be certified differs slightly by statute, but all statutes provide that one ground for certification is that, in the judgment of the certifying official, prosecution by the United States is in the public interest and necessary to secure substantial justice.<sup>17</sup> The

---

<sup>9</sup> § 249.

<sup>10</sup> See § 249(a)(1).

<sup>11</sup> See § 249(a)(2).

<sup>12</sup> See § 249(a)(3).

<sup>13</sup> § 3631.

<sup>14</sup> § 245.

<sup>15</sup> § 247.

<sup>16</sup> See §§ 245(a)(1), 247(e), 249(b)(1).

<sup>17</sup> Section 249 states that no person may be prosecuted unless the Attorney General or an authorized designee certifies in writing that: (A) the state does not have jurisdiction; (B) the state has requested that the Federal Government assume jurisdiction; (C) the verdict or sentence obtained pursuant to state charges left demonstratively unvindicated the Federal interest in eradicating bias-motivated violence; or (D) a prosecution by the United States is in the public interest and necessary to secure substantial justice. § 249(b)(1). Section 245 requires that the Attorney General, Deputy Attorney General, Associate Attorney General, or a specially designated Assistant Attorney General certify that the prosecution is in the public interest and necessary to secure substantial justice. § 245(a)(1). Section 247 requires certification by the “Attorney General or his designee that in his judgment a prosecution by the United States is in the public interest and necessary to secure substantial justice.” § 247(e).

authority to issue certifications has been delegated to the Assistant Attorney General for Civil Rights Division.<sup>18</sup>

## **A. 18 U.S.C. § 249: The Matthew Shepard and James Byrd, Jr., Hate Crimes Prevention Act**

### **1. Overview**

The newest federal hate crime statute, the Matthew Shepard and James Byrd, Jr., Hate Crimes Prevention Act, 18 U.S.C. § 249,<sup>19</sup> prohibits willfully causing bodily injury—or attempting to cause bodily injury with a dangerous weapon—if the defendant is motivated by the actual or perceived race, color, religion, national origin, gender, gender identity, sexual orientation, or disability of any person.<sup>20</sup> Section 249, which was signed into law in 2009, covers more bias motivations than had been covered by then-existing federal hate crime laws. Unlike earlier enacted federal hate crime statutes, § 249 applies to hate crimes committed because of gender identity and sexual orientation. Moreover, § 249 eliminates requirements, present in other statutes, that prosecutors prove that the victim was engaging in a federally-protected activity, such as enjoying housing rights (required by 42 U.S.C. § 3631) or other enumerated rights (required by 18 U.S.C. § 245). It is thus less complicated to prove in court than earlier enacted statutes.

Section 249, however, has limitations; therefore, federal prosecutors continue to prosecute defendants using other federal hate crime statutes where appropriate. First, § 249 does not apply to threats, so cases involving threats, including particularly virulent, symbolic threats like cross-burnings, must be prosecuted using other federal hate crime statutes. Second, § 249 cannot be used if a prosecutor seeks the death penalty, as it is not a death-eligible offense.<sup>21</sup>

### **2. Elements**

Section 249 has three subsections that differ in the type of bias motivation they prohibit and the number of elements a prosecutor must establish. All three subsections require proof that the defendant willfully caused bodily injury or attempted to cause bodily injury using a firearm, fire, explosive or incendiary device, or other dangerous weapon. An attempt to cause bodily injury *without* using such a dangerous weapon is not subject to prosecution under § 249. Thus, if a defendant swings at a victim with his *fists* and misses, § 249 is not implicated, even if it is clear that the attempted assault was motivated by bias. The same action, taken with a knife in the victim's hand, would constitute an attempt subject to prosecution under § 249.

---

<sup>18</sup> See 28 CFR § 0.50 (2011) (delegating authority for §§ 245 and 249); AG Order, 2048-96, Delegation of Authority to Authorize the Initiation of Prosecutions under § 247 (delegating authority for § 247).

<sup>19</sup> § 249.

<sup>20</sup> The statute explicitly states that prosecution may be undertaken if the crime is committed because of the characteristic of any person—not just the victim. Thus, for example, if a skinhead assaults a white man for marrying a woman of color, the crime is prosecutable even though the assault was not motivated by the race of the person who was subject to the attack.

<sup>21</sup> A violation of § 249 is always a felony offense. A conviction under § 249 carries a statutory maximum of ten years' imprisonment. § 249(a)(1)(A). If death results, or if the defendant's actions include kidnapping or attempted kidnapping, sexual abuse or attempted sexual abuse, or an attempt to kill, the offense is punishable by imprisonment for any term of years or for life. § 249(a)(1)(B). The statute of limitations is seven years unless death results, in which case there is no statute of limitations. § 249(d).

### a. Section 249(a)(1)

*A young man of the Navajo Nation stopped in at a fast-food restaurant in Farmington, New Mexico. While there, the young man, who had a developmental disability, was apparently befriended by the defendants, three white restaurant workers, who lured him to one of their apartments. While the victim was at the apartment, the defendants convinced him to let them draw on his back. Although they told him they were going to draw “feathers” and “native pride” in an apparent reference to his Native American heritage, they instead drew satanic and anti-gay images. Then they shaved his head, leaving his remaining hair in the shape of a swastika, outlined it with a marker, and wrote “KKK” and “white power” within the swastika. Finally, they heated a wire hanger on the stove and used it to burn the victim’s flesh, branding a swastika into his arm, causing bodily injury. During the ordeal, they used the victim’s cognitive disability to persuade him to say he “consented” to some of the acts.<sup>22</sup>*

The subsection of § 249 used to prosecute the defendants in the above case is § 249(a)(1), which prohibits willfully causing bodily injury, or attempting to do so with a weapon, if the assault is undertaken because of the actual or perceived race, color, religion or national origin of any person. Although the express wording of the statute includes “religion” and “national origin” without limitation, as will be explained, due to jurisdictional limitations, this subsection of the statute may be used only to prosecute crimes motivated by certain religions and national origins. All that a prosecutor must prove to establish a violation of § 249(a)(1) is violent conduct and the relevant bias motivation. As explained above, they need not show an intent to interfere with a federally-protected right (as they must to prove a violation of other federal hate crime statutes). They also need not prove a link to interstate commerce, which, as explained below, they must do to establish a violation of § 249(a)(2).<sup>23</sup> Congress passed subsection (a)(1) under power granted to it by the Thirteenth Amendment, which authorizes Congress to pass legislation to remedy racial injustices.<sup>24</sup> Because § 249(a)(1) was enacted pursuant to the Thirteenth Amendment, a prosecutor need prove no link to interstate commerce or any other jurisdictional hook for federal jurisdiction to attach.

While some might believe the Thirteenth Amendment is limited to ensuring freedom to those held in slavery before the civil war and that it therefore empowers Congress to act only on behalf of African Americans (i.e., the victims of chattel slavery), the Thirteenth Amendment has not been given such a narrow construction. Rather, it “was a charter of universal civil freedom for all persons, of whatever race, color, or estate, under the flag.”<sup>25</sup> For this reason, Congress has broad Thirteenth Amendment authority to protect all racial groups; therefore, Native American victims, like the victim in *United States v. Hatch*,<sup>26</sup> or white victims or Hispanic victims, fall under the protections of Thirteenth Amendment legislation.

Section 249(a)(1) explicitly states that it applies not only to conduct motivated by race and color, but also to conduct motivated by religion and national origin. This is so because Congress is empowered

---

<sup>22</sup> See *United States v. Hatch*, 722 F.3d 1193, 1195-96 (10th Cir. 2013); *Brief for the United States*, *United States v. Hatch*, 2012 WL 3886568, 5-6 (10th Cir. 2012).

<sup>23</sup> For this reason, in the *Hatch* case described above, prosecutors proceeded under the first subsection of § 249, and charged that the defendants’ violent conduct was motivated by the victim’s race (i.e., Native American). Because the victim was developmentally disabled, prosecutors might also have considered charging the defendants under § 249(a)(2). But, as explained in the discussion of subsection § 249(a)(2) below, doing so would have required prosecutors to prove not only that the defendants were motivated by the victim’s disability, but also an *additional* element—a nexus to the Commerce Clause.

<sup>24</sup> *Jones v. Alfred H. Mayer Co.*, 392 U.S. 409, 440 (1968) (holding that Congress has broad power under § 2 of the Thirteenth Amendment to identify the “badges and incidents of slavery” and enact legislation to combat them).

<sup>25</sup> *Bailey v. Alabama*, 219 U.S. 219, 240-41 (1911).

<sup>26</sup> *Hatch*, 722 F.3d at 1201-06.

by the Thirteenth Amendment to enact legislation to protect any group which was considered to be “racial” at the time the amendment was passed, even if that characteristic is presently considered to be a religious characteristic (e.g., Judaism)<sup>27</sup> or a national origin characteristic (e.g., Arab)<sup>28</sup> rather than a racial characteristic. Congress expressly invoked this power in enacting § 249(a)(1).<sup>29</sup>

It is important to note, however, that § 249(a)(1) cannot be used to prosecute violent conduct motivated by a person’s religion or national origin if that religion or national origin was not considered a race at the time the Thirteenth Amendment was enacted. For example, because Baptists in 1865 were considered to be members of a religion rather than a race, if a defendant targeted a victim because he or she is a Baptist, the defendant could not be prosecuted under § 249(a)(1). In such a situation, prosecutors should proceed under §§ 249(a)(2) or (a)(3) if the jurisdictional elements of those subsections are supported by the evidence.

The constitutionality of § 249(a)(1) has been upheld by three courts of appeals and several district courts.<sup>30</sup> The attached appendix provides a circuit-by-circuit summary of § 249(a)(1) cases issued to date.

## **b. Section 249(a)(2)**

*17-year old Mercedes Williamson, who identified as female even though she had been assigned a male gender at birth, was open about her gender identity. She had a consensual sexual relationship with the defendant, Josh Vallum, who knew of her transgender status. Vallum was a member of a gang that forbade “homosexual” relationships, and Vallum kept the nature of his relationship with Ms. Williamson secret. In 2014, he ended his relationship with her and had no contact with her until he learned that one of his friends knew or suspected that she was transgender. At that point, he decided to kill her.*

*On May 29, 2015, Vallum picked up Ms. Williamson in Alabama, planning to take her to Mississippi and kill her there. He drove Ms. Williamson from Alabama to his father’s residence in Mississippi. While Ms. Williamson still sat in the passenger seat of Vallum’s car after the trip, he assaulted her. He first used a stun gun to electrically shock her in the chest. Then he repeatedly stabbed her with a 75th Ranger Regiment pocket knife.*

*Ms. Williamson, injured, fled from the vehicle. Vallum chased her and stabbed her again multiple times. Vallum delivered what he believed to be a fatal stab to Ms. Williamson’s head, as he thought he “hit brain” with a blow from the pocket knife. Ms. Williamson briefly got back up but again fell to the ground. Vallum went back to his vehicle to attend to a cut on his thumb that he inadvertently inflicted with his own knife during the attack. At that time, Ms. Williamson got up again and stumbled farther into the woods.*

---

<sup>27</sup> See *Shaare Tefila Congregation v. Cobb*, 481 U.S. 615, 617 (1987) (holding Jews are a race for purposes of 42 U.S.C. § 1982).

<sup>28</sup> See *Saint Francis College v. Al-Khazraji*, 481 U.S. 604, 613 (1987) (holding Arabs are a race for purposes of 42 U.S.C. § 1981).

<sup>29</sup> See National Defense Authorization Act For Fiscal Year 2010, Pub. L. No. 111-84, 123 Stat 2190, *reprinted* in 18 U.S.C. § 242 (2012) Notes, Findings (8) (“Both at the time when the 13th, 14th, and 15th amendments to the Constitution of the United States were adopted, and continuing to date, members of certain religious and national origin groups were and are perceived to be distinct ‘races.’ Thus, in order to eliminate, to the extent possible, the badges, incidents, and relics of slavery, it is necessary to prohibit assaults on the basis of real or perceived religions or national origins, at least to the extent such religions or national origins were regarded as races at the time of the adoption of the 13th, 14th, and 15th amendments to the Constitution of the United States.”).

<sup>30</sup> *United States v. Cannon*, 750 F.3d 492, 505 (5th Cir. 2014); *Hatch*, 722 F.3d at 1201; *United States v. Maybee*, 687 F.3d 1026, 1030 (8th Cir. 2012); *United States v. Roof*, 225 F. Supp. 3d 438, 450 (D.S.C. 2016); *United States v. Metcalf*, No. 15-CR-1032-LRR, 2016 WL 827763, at 4 (N.D. Iowa Mar. 2, 2016); *United States v. Henery*, 60 F. Supp. 3d 1126, 1132 (D. Idaho 2014).

*Vallum retrieved a hammer from the trunk of his vehicle and chased after Ms. Williamson. He caught up with Ms. Williamson and hit her on the back of the head with the hammer. Ms. Williamson fell to the ground and Vallum used the hammer to hit her in the head several more times until she was dead.*

*After killing Ms. Williamson, Vallum attempted to dispose of the murder weapons and other evidence linking him to the crime. He also falsely claimed to law enforcement that he killed Ms. Williamson in a panic after discovering that she was transgender.*

*Vallum pleaded guilty on December 21, 2016, becoming the first defendant to be convicted for violating § 249 based upon a crime against a transgender victim. In pleading guilty, Vallum acknowledged not only that he was responsible for Ms. Williamson's death, but also that he had previously lied about the circumstances surrounding it. He also admitted that he would not have killed Ms. Williamson if she had not been transgender. On May 15, 2017, Vallum was sentenced to 49 years in federal prison. In July 2016, he had received a life sentence in state court.<sup>31</sup>*

*Vallum was prosecuted under the second subsection of § 249, section 249(a)(2),<sup>32</sup> which prohibits willfully causing bodily injury, or attempting to cause bodily injury with a dangerous weapon, if the defendant is motivated by the actual or perceived national origin, gender, sexual orientation, gender identity, or disability of any person, and if the crime is in, or affecting, interstate or foreign commerce in one of the ways set forth by statute.*

Section 249(a)(2) prohibits violent conduct motivated by non-racial characteristics such as gender, disability, sexual orientation, and—as in the case of Mercedes Williamson—gender identity. It also prohibits violent conduct motivated by bias against religions and national origins which were not considered to be races at the time the Thirteenth Amendment was passed. For example, the Department has prosecuted a case involving victims who are members of the Amish religion under this provision, although the § 249 convictions were reversed due to jury instructions found erroneous under a Supreme Court case decided after the date that the case was tried.<sup>33</sup>

Section 249(a)(2) was enacted pursuant to Congress's power to regulate interstate commerce.<sup>34</sup> To prove a violation of § 249(a)(2), federal prosecutors must prove not only that the defendant engaged in violent conduct motivated by bias towards a group identified in the subsection of the statute, but also that the offense was in or affecting commerce. The principal author of the Shepard-Byrd Act has noted that, in passing § 249(a)(2), Congress intended to legislate to the fullest extent of its Commerce Clause power.<sup>35</sup>

Congress expressly enumerated in § 249 several ways that prosecutors may meet their burden of establishing that an offense was in or affected interstate commerce.<sup>36</sup> These include (1) travel of the defendant or the victim across a State line or national border in connection with the offense; (2) travel of the defendant or the victim using a channel, facility, or instrumentality of interstate or foreign commerce in connection with the offense; (3) use of a channel, facility, or instrumentality of interstate or foreign commerce in connection with the offense; (4) use, in the offense, of a dangerous weapon that has traveled

---

<sup>31</sup> United States v. Vallum, No. 116CR00114, WL 8969558 (S.D.Miss. 2016); *see* <https://www.justice.gov/opa/pr/mississippi-man-sentenced-49-years-prison-bias-motivated-murder-transgender-woman-lucedale>; <https://www.fbi.gov/news/stories/historic-hate-crime-sentencing>.

<sup>32</sup> § 249(a)(2).

<sup>33</sup> *See* United States v. Miller, 767 F.3d 585, 591-92 (6th Cir. 2014).

<sup>34</sup> *See* U.S. CONST. art. I, § 8, cl. 3.

<sup>35</sup> *See* 155 CONG. REC. S10772, S10773 (daily ed. Oct. 27, 2009) (statement of Sen. Patrick Leahy) (“I want to note that the sponsors and supporters intend with its passage, to authorize Federal investigations and prosecutions of those hate crimes described to the fullest extent permitted by the Constitution.”).

<sup>36</sup> *See* § 249(a)(2)(B).

in interstate or foreign commerce; (5) interference with commercial or other economic activity in which the victim is engaged at the time of the offense; or (6) conduct otherwise affecting interstate or foreign commerce.<sup>37</sup> In the prosecution of Vallum, the defendant admitted through his plea that he had lured his victim into his car and traveled across state lines during the offense. This admission established federal jurisdiction under subsection (a)(2)(B)(i).<sup>38</sup> Had the case gone to trial, prosecutors might also have sought to establish federal jurisdiction by introducing evidence that at least one of the weapons traveled in interstate or foreign commerce, which would satisfy subsection (a)(2)(B)(iii).

The constitutionality of § 249(a)(2) has been upheld by several district courts.<sup>39</sup> The attached appendix provides a circuit-by-circuit summary of § 249(a)(2) cases issued to date.

### c. Section 249(a)(3)

Section 249(a)(3)<sup>40</sup> prohibits causing bodily injury, or attempting to cause bodily injury with a weapon, if the attack is undertaken because of race, color, religion, national origin, gender, gender identity, sexual orientation, or disability, *and* if the crime occurred in the Special Maritime and Territorial Jurisdiction of the United States.<sup>41</sup> In Section 7 of Title 18, Congress precisely defined what constitutes the Special Maritime and Territorial Jurisdiction.<sup>42</sup> This definition generally includes the high seas and lands over which the federal government has exclusive or concurrent jurisdiction. This does not automatically include federal prisons.<sup>43</sup>

## B. 42 U.S.C. § 3631: Criminal Provisions of the Fair Housing Act

*A white couple, along with the woman's three bi-racial children and the children's African-American grandfather, moved into a rented home in a predominantly white neighborhood in Indiana. After a night of heavy drinking, two men built a cross, took it to the couple's home, dug a hole in their yard approximately five feet from the room in which two of the children were sleeping, planted the cross, doused it with gasoline, set it on fire, laughed, and then took pictures while they watched it burn; one of the men shared the pictures with his friends and bragged that he "had burned a cross on a n\*gger's yard." The family, terrified for the children's safety, eventually moved from the neighborhood.*<sup>44</sup>

---

<sup>37</sup> *Ibid.*

<sup>38</sup> § 249(a)(2)(B)(i).

<sup>39</sup> See *United States v. Gardner*, 993 F. Supp. 2d 1294, 1305 (D. Or. 2014); *United States v. Mason*, 993 F. Supp. 2d 1308 (D. Or. 2014); *United States v. Jenkins*, 909 F. Supp. 2d 758, 767-68 (E.D. Ky. 2012); *United States v. Mullet*, 868 F. Supp. 2d 618, 621 (N.D. Ohio 2012), conviction overturned on other grounds, *United States v. Miller*, 767 F.3d 585, 590 (6th Cir. 2014) (holding jury instructions were infirm under law that issued while case was on appeal). One court struck down subsection (a)(2) in an as-applied challenge under the Commerce Clause, *United States v. Hill*, 182 F. Supp. 3d 546 (E.D. Va. 2016), but the decision was reversed on the ground that it was premature to dismiss the case before facts had been developed at trial, *United States v. Hill*, No. 16-4299, 2017 WL 3575241, at 2 (4th Cir. Aug. 18, 2017).

<sup>40</sup> § 249(a)(3).

<sup>41</sup> Article III, § 2 of the Constitution grants Congress the authority to extend the federal judicial power to federal lands and the high seas. U.S. CONST. art. III, § 2, cl. 1; *Southern Pac. Co. v. Jensen*, 244 U.S. 205 (1917) ("It is not questioned that whatever may be necessary to the full and unlimited exercise of admiralty and maritime jurisdiction is in the government of the Union. Congress may pass all laws which are necessary and proper for giving the most complete effect to this power.").

<sup>42</sup> See 18 U.S.C. § 7 (2012).

<sup>43</sup> See *United States v. Davis*, 726 F.3d 357, 362 (2d Cir. 2013) (explaining that not all lands owned by the federal government within a state are rendered, by that fact alone, within the SMTJ of the United States and holding that absent a showing that the federal government had obtained land by consent or cessation, land was not in the SMTJ).

<sup>44</sup> *United States v. Milbourn*, 600 F.3d 808 (7th Cir. 2010).

The defendant was convicted of violating, among other statutes, the criminal provision of the Fair Housing Act, codified at 42 U.S.C. § 3631,<sup>45</sup> which prohibits housing-related threats and violence.

## 1. Overview

To prove a defendant guilty of violating § 3631, the government must prove that the defendant used or threatened to use force to willfully interfere with a victim because of the victim's race, color, religion, sex, handicap, familial status, or national origin, and because the victim was enjoying one of the housing rights set forth in the statute.<sup>46</sup>

Passage of § 249 (outlined above) has decreased the use of § 3631, particularly in racial-bias cases involving actual physical violence. If a defendant, motivated by race, uses physical force to interfere with a housing right, then both § 3631 and § 249 are implicated. To prove a violation of § 3631, the prosecutor will need to establish the defendant's motive to interfere with a particular housing right. But to prove a violation of § 249(a)(1), the prosecutor will have to establish only the defendant's racial-bias motivation and that the defendant willfully caused bodily injury or attempted to do so with a dangerous weapon. In cases involving other kinds of bias listed in § 3631, however, the calculus may be different. In a case in which a defendant used force and violence to interfere with a housing right due to gender, disability, or a religion or national origin that cannot form the basis of a prosecution under § 249(a)(1), both § 249(a)(2) and § 3631 are implicated. In such a case, it may be simpler for the jury to understand the case as a violation of a victim's housing rights than to prove an effect on interstate commerce.

Moreover, as discussed above, § 249 contains a significant limitation as compared to other federal statutes in that it has no threat provision. Section 3631 thus remains a useful federal hate crime charge to bring in cases involving threats of force. Threats made at a person's home can be particularly disquieting as the home is where people generally gather to relax and escape the stress that besets them in other aspects of their lives. Because cross-burnings are often committed outside of homes and are a particularly virulent form of threat, § 3631 is the most often charged federal statute in cross-burning cases.<sup>47</sup> Violations of the statute may also be charged in cases of verbal threats or written threats, whether delivered by mail, in electronic format, or by hand. But because § 3631 does not apply to crimes motivated by someone's sexual orientation or gender identity, it leaves a gap in federal hate crime coverage.

## 2. Elements

In order to establish a violation of § 3631, the government must prove the following elements: (1) the defendant used or threatened force; (2) the defendant willfully injured, intimidated or interfered with (or attempted to injure, intimidate or interfere with) a victim; (3) the defendant acted because of the victim's race, color, religion, sex, handicap, familial status, or national origin; and, (4) the

---

<sup>45</sup> § 3631.

<sup>46</sup> *Ibid.*

<sup>47</sup> Despite its frequent use in prosecuting crimes arising from cross-burnings, § 3631 should not be thought of as a "cross-burning" statute. If a cross is burned to interfere with some other federally-protected right rather than to interfere with housing rights, then the crime would not violate the Fair Housing statute. For example, if a defendant burns a cross to intimidate African-American students and interfere with their right to attend a public school, then his actions would violate § 245(b)(2)(A). If a defendant burns a cross at a historically black church to interfere with worshipers there, then his actions would violate § 247(a)(2). Moreover, if an individual burns a cross, not to intimidate but, instead, to show pride and solidarity, such as when it is done only in front of like-minded Klan members on Klan property, then the individual's actions are considered protected speech. *See Virginia v. Black*, 538 U.S. 343, 366 (2003) (noting that burning a cross at a political rally would almost certainly be protected expression, as might burning a cross in a play or movie (e.g., as in *Mississippi Burning*)).

defendant acted because the victim was enjoying one of the housing rights set forth in the statute—the most common being the victim’s occupation of a dwelling.<sup>48</sup>

### **a. Force or Threat of Force**

The first element that the government must prove is that the defendant used force or the threat of force. “Force” means power, violence, compulsion, or restraint exerted upon or against a person or thing.<sup>49</sup>

Threats “encompass those statements where the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence to a particular individual or group of individuals.”<sup>50</sup> A threat of force means a communication made through words, gestures, or symbolic speech, to inflict a threat of death or bodily harm.<sup>51</sup> The government need not prove that the defendant actually meant to carry out the threat.<sup>52</sup> Whether a defendant’s words and actions constitute a threat is a question for the trier of fact.<sup>53</sup>

### **b. Willfully Injuring, Intimidating, or Interfering with Another**

The government must also prove that the defendant willfully injured, intimidated, or interfered with the victim or attempted to do so. The words “injure,” “intimidate,” and “interfere with” cover a variety of conduct intended to harm, frighten, prevent, or punish the free action of others.<sup>54</sup> The central question is whether the defendant intended to injure, intimidate, or interfere with the victims, not whether the defendant succeeded in doing so.<sup>55</sup> Proof that the defendant’s conduct actually intimidated the victims or drove them from their home is unnecessary.<sup>56</sup> Nevertheless, proof that the defendant’s conduct actually did interfere with or intimidate a victim may provide additional evidence that the defendant intended to interfere with or intimidate that victim.<sup>57</sup>

### **c. Because of Race, Color, Religion, Sex, Handicap, Familial Status, or National Origin**

The government must establish that the defendant acted “because of” a protected characteristic set forth in the statute: race, color, religion, sex, handicap, familial status, or national origin. Two of these terms are specifically defined in the Fair Housing Act. Under the Act, “handicap” means: (1) a physical or mental impairment which substantially limits one or more of such person’s major life activities; (2) a

---

<sup>48</sup> § 3631.

<sup>49</sup> See *Johnson v. United States*, 559 U.S. 133, 138-39 (2010) (interpreting 18 U.S.C. § 924(e)(2)(B)(i) by recognizing that “force has a number of meanings,” noting that in its “more general usage it means strength or energy; active power; vigor; often an unusual degree of strength or energy, power to affect strongly in physical relations, or power, violence, compulsion, or constraint exerted upon a person,” and observing that *Black’s Law Dictionary* “defines ‘force’ as power, violence, or pressure directed against a person or thing”) (internal citations, quotations, and alterations omitted). Use of force thus includes all acts of physical violence. See also *United States v. Bamberger*, 452 F.2d 696, 699 (2d Cir. 1971) (discussing and relying on Webster’s definition of force).

<sup>50</sup> *Virginia v. Black*, 538 U.S. 343, 359 (2003) (defining “true threats”); *United States v. Dutcher*, 851 F.3d 757, 761 (7th Cir.) (explaining *Virginia v. Black*), cert. denied, No. 16-9610, 2017 WL 2654689 (U.S. Oct. 2, 2017).

<sup>51</sup> *United States v. Magleby*, 420 F.3d 1136, 1139 (10th Cir. 2005).

<sup>52</sup> *Dutcher*, 851 F.3d at 761.

<sup>53</sup> *United States v. Wheeler*, 776 F.3d 736, 742 (10th Cir. 2015).

<sup>54</sup> *United States v. McDermott*, 29 F.3d 404, 408-09 (8th Cir. 1994) (approving jury instruction using similar language).

<sup>55</sup> *United States v. Hayward*, 6 F.3d 1241, 1252 (7th Cir. 1993).

<sup>56</sup> *United States v. Redwine*, 715 F.2d 315, 322 (7th Cir. 1984) (“[I]nterference or intimidation is to be inferred from violent acts or threats, and there is no need to show the subjective state of mind of the intended victim.”).

<sup>57</sup> See *United States v. Magleby*, 241 F.3d 1306, 1311 (10th Cir. 2001) (holding that a jury may properly consider victims’ reaction when assessing defendant’s intent to violate housing rights by burning a cross).

record of having such an impairment; or (3) being regarded as having such an impairment.<sup>58</sup> The term “familial status” “refers to the presence of minor children in the household.”<sup>59</sup>

#### **d. Because of a Housing Right**

The government must also establish that the defendant acted because of a housing right. The housing rights protected by the statute include: (1) selling, purchasing, renting, financing, or occupying a dwelling; (2) contracting or negotiating to do so; (3) applying for, or participating in, a service, organization, or facility relating to the business of selling or renting dwellings; (4) affording other persons the ability to participate in such activities; and, (5) aiding or encouraging other persons to participate in such activities.<sup>60</sup> The broadest of these terms, and the one most frequently used in indictments, is a person’s right to “occupancy.” The activities covered by the term “occupancy” include associating with persons of another race inside one’s dwelling.<sup>61</sup>

Although the occupancy requirement means that most cases arising under § 3631 are ones that occur at or near the victim’s dwelling, it is not a requirement.<sup>62</sup> There is no requirement that the government prove that the defendants intended to force the victims to move from their homes or neighborhood. It must prove only that the defendants wanted to interfere with one of the statute’s enumerated housing rights. However, if the victims did move (or if they searched for alternative housing) because of the defendant’s actions, this may be powerful evidence that the defendant’s conduct interfered with their housing right. The attached appendix provides a circuit-by-circuit summary of § 3631 cases issued to date.

### **C. 18 U.S.C. §§ 245(b)(2), (4), and (5): Federally-Protected Activities**

*In March 2005, the defendants, two young men who were both high and driving around Kansas City in a series of stolen vehicles with a female friend, searched for an African American to shoot after one of the men, Steven Sandstrom, bragged to the other man, Gary Eye, that he had shot at, but missed hitting, a “n\*gger” in a convenience store earlier in the evening. Using additional racial slurs, Sandstrom and Eye then bragged to each other about their desire and ability to kill African Americans. Early the next morning while still driving the streets of Kansas City, they saw William McCay, an African-American man, walking alone along a city street. While Sandstrom drove past McCay, Eye fired at McCay but missed. They then drove back toward McCay where Sandstrom pulled the car over so Eye could approach McCay on foot. Eye walked up to*

---

<sup>58</sup> 42 U.S.C. § 3602(h) (2012).

<sup>59</sup> Gilligan v. Jamco Development Corp., 108 F.3d 246, 247 (9th Cir. 1997) (interpreting 42 U.S.C. § 3602(k)).

<sup>60</sup> § 3631(a).

<sup>61</sup> See, e.g., United States v. Hayward, 6 F.3d 1241 (7th Cir. 1993) (upholding application of § 3631 where cross was burned in front of house of white family that hosted black friends), overruled on other grounds by United States v. Colvin, 353 F.3d 569 (7th Cir. 2003) (en banc); United States v. Wood, 780 F.2d 955, 961 (11th Cir. 1986) (“Section 3631 was clearly designed to protect an individual’s right to occupy a dwelling of one’s choice free from racial pressure. This right, however, means very little if the occupant’s physical safety inside that dwelling is contingent upon his refraining from associating with members of another race.”).

<sup>62</sup> See, e.g., United States v. Piekarsky, 687 F.3d 134, 148 (3d Cir. 2012) (“Viewing [evidence that during the attack the defendants yelled that the victim should get out of “our town” and get out of Shenandoah]—coupled with the other testimony about the Defendants’ general dislike of Hispanic or Latino individuals moving into Shenandoah, . . . we conclude that a reasonable juror could rationally conclude that the nature of the beating, . . . the extent of the violence involved in this case, and the gratuitous nature of the racial epithets . . . were, taken together, indicative that [the defendants] intended to injure [the victim] with the purpose of intimidating him, or other Hispanic or Latino individuals, from residing in Shenandoah.”).

*McCay, struggled briefly with him, and then fired a shot—killing him. Eye then returned to the car and the two men drove away.*<sup>63</sup>

This case, which occurred prior to the passage of § 249, was charged as a violation of 18 U.S.C. § 245(b)(2)(B).<sup>64</sup> The defendants were charged with, among other civil rights and weapons offenses, using force to willfully interfere with the victim because of his race and because of his use of the street, a facility provided and administered by Kansas City. Each was sentenced to life imprisonment.

## 1. Overview

Before Congress passed 18 U.S.C. § 249, § 245 was the federal hate crime statute that covered the broadest range of activities. The primary portion of the statute used in civil rights prosecutions is subsection (b)(2), which prohibits using force or threats to interfere with various enumerated activities because of race, color, religion, or national origin.

Since Congress passed § 249, § 245 is rarely used to prosecute cases involving the use of force. If the physical assault was based upon race, color, or one of the religions or national origins that fall under § 249(a)(1), it is more straightforward for a prosecutor to file charges under § 249(a)(1) and to show that the defendant willfully caused bodily injury or attempted to do so with a dangerous weapon, and that the defendant acted because of the relevant characteristic. If the assault was based upon one of the national origins or religions that falls under § 249(a)(2), a prosecutor is still more likely to prove a connection to interstate commerce, as is required by § 249(a)(2), see *infra*, than to prove that the defendant acted because of the victim's use or enjoyment of one of the federally-protected activities listed in the statute. Because § 249 lacks a threat provision, however, § 245 remains useful in cases in which a threat is made. If the threat is unrelated to a housing right and is therefore not covered by 42 U.S.C. § 3631, then prosecutors must determine whether the threat may be prosecutable under § 245. In such a situation, the prosecutor should examine whether he or she can prove that the defendant intended to interfere with one of the rights set forth in the statute. However, because § 245(b)(2) does not cover threats based upon gender, sexual orientation, gender identity, or disability status, there is a gap in its coverage.

The constitutionality of § 245 has been upheld as a valid exercise of Congress's power under both the Commerce Clause and the Fourteenth Amendment, but the Fourteenth Amendment basis has been abandoned in light of the Supreme Court's decision in *United States v. Morrison*,<sup>65</sup> which limited the reach of the Fourteenth Amendment—and thus Congress's ability to enact enabling legislation under Section 5 of that Amendment—to conduct that involves some degree of state action.<sup>66</sup> Section 245 has, however, been upheld as a valid exercise of Congress's power under the Thirteenth Amendment because it, unlike the Fourteenth Amendment, “reaches purely private conduct.”<sup>67</sup> The attached appendix provides a circuit-by-circuit summary of § 245 cases issued to date.

---

<sup>63</sup> See *United States v. Sandstrom*, 594 F.3d 634 (8th Cir. 2010).

<sup>64</sup> § 245(b)(2)(B).

<sup>65</sup> *United States v. Morrison*, 529 U.S. 598 (2000).

<sup>66</sup> See *United States v. Nelson*, 277 F.3d 164, 175 n.10 (2d Cir. 2002).

<sup>67</sup> *Id.* at 175. For other cases upholding § 245 as a valid exercise of either Commerce Clause or Thirteenth Amendment authority, see *United States v. Allen*, 341 F.3d 870, 879-85 (9th Cir. 2003) (finding § 245 to be a valid exercise of Congress's power under both the Commerce Clause and the Thirteenth Amendment); *United States v. Lane*, 883 F.2d 1484, 1493 (10th Cir. 1989) (“If in an effort to rid interstate commerce of the burdens imposed on it by racial discrimination Congress may prohibit a person from denying another person equal employment opportunities by refusing to hire him or by firing him solely because of his race, then Congress may also prohibit a person from denying another person equal employment opportunities because of his race by violently injuring or killing him.”); *United States v. Bledsoe*, 728 F.2d 1094, 1097 (8th Cir. 1984) (finding it clear that under the Thirteenth Amendment, Congress could reach purely private action and reasoning that there can be no “doubt that

## 2. Elements

In order to establish a violation of § 245(b)(2),<sup>68</sup> the government must prove beyond a reasonable doubt that: (1) the defendant used force or the threat of force; (2) the defendant willfully injured, intimidated, or interfered with a person, or attempted to do so; (3) the defendant acted because of that person's race, color, religion, or national origin; and, (4) the defendant acted because that person was enjoying one of the rights protected by the statute. Those rights are set forth below.

### a. Federally Protected Activities

- |                |   |
|----------------|---|
| I. (b)(2)(A)   | II. Attending or enrolling in public school or college <sup>69</sup>  |
| III. (b)(2)(B) | IV. Participating or enjoying a benefit, service, privilege, program, facility or activity provided or administered by a State or its subdivision <sup>70</sup>                                 |
| V. (b)(2)(C)   | VI. Applying for or enjoying state or private employment <sup>71</sup>  |
| VII. (b)(2)(D) | VIII. Serving on a state jury or attending state court in connection with such service <sup>72</sup>  |
| IX. (b)(2)(E)  | X. Traveling or using a facility or interstate commerce or common carrier <sup>73</sup>   |
| XI. (b)(2)(F)  | XII. Enjoying the goods, services, facilities, privileges, advantages or accommodations of hotels, restaurants, theaters, concert halls, sports arenas, or similar establishments <sup>74</sup> |

### b. Assisting and Supporting Others in Obtaining Benefits and Rights

Section 245(b)(1)<sup>75</sup> prohibits using force or threats to deprive individuals of the enjoyment of certain federally-protected activities (e.g., voting, applying for/serving in federal employment, serving on a jury, receiving federal benefits) without regard to whether the defendant was motivated by bias or some other motive. Thus, if a defendant uses violence to interfere with a victim's access to federal benefits (e.g., social security benefits), it is a violation of subsection (b)(1)(B)<sup>76</sup> regardless of whether the defendant was motivated by the victim's race or whether the defendant had a purely financial motive. If, however, a defendant interferes with one of the federally-protected activities enumerated in the statute and is motivated by discriminatory animus (such as race, color, religion, or national origin), then the case may be prosecutable under subsection (b)(4) or (b)(5) of § 245,<sup>77</sup> provided the prosecutor establishes the bias motivation.

In essence, this means that § 245 separately prohibits the forceful infringement of rights identified in subsection (b)(1), whenever such interference is motivated by animus. There is a strategic question prosecutors must consider about whether, in such cases, a prosecution is better brought under subsection

---

interfering with a person's use of a public park because he is black is a badge of slavery"); *United States v. Furrow*, 125 F. Supp. 2d 1178, 1183 (C.D. Cal. 2000) (upholding the constitutionality of § 245 under the Commerce Clause).

<sup>68</sup> § 245(b)(2).

<sup>69</sup> § 245(b)(2)(A).

<sup>70</sup> § 245(b)(2)(B).

<sup>71</sup> § 245(b)(2)(C).

<sup>72</sup> § 245(b)(2)(D).

<sup>73</sup> § 245(b)(2)(E).

<sup>74</sup> § 245(b)(2)(F).

<sup>75</sup> § 245(b)(1).

<sup>76</sup> § 245(b)(1)(B).

<sup>77</sup> § 245(b)(4) or (b)(5).

(b)(1) or whether proceeding under subsections (b)(4) and (b)(5) would be better. If a case is brought under subsection (b)(1), then the prosecution need not prove racial bias. For this reason, it is technically easier to prove a violation of subsection (b)(1) than it is to prove a violation of subsection (b)(4) or (b)(5). If the evidence of racial motivation is strong, however, and the prosecutor wants to ensure that the evidence is before the jury, the prosecutor may choose to pursue charges under subsection (b)(4) or (b)(5). This would allow for the application of a hate crime motivation adjustment at sentencing (see *infra*) and to characterize the violation as a hate crime.

In addition, subsections (b)(4) and (5)<sup>78</sup> allow prosecutors to extend the reach of the statute to prosecute those assisting others, or peacefully protesting on behalf of others, to obtain the statutorily enumerated benefits. For example, if a defendant used force or violence to prevent a white civil rights worker from joining in a voting drive to help African Americans register to vote, the statute would be implicated, even if there was no proof that the victim was targeted due to his or her race (or other protected characteristic). Similarly, the statute would be implicated if a defendant used force or violence to target a victim who was peacefully opposing, through speech or assembly, the fact that an individual or group of individuals had been denied the opportunity to receive or participate in any of the enumerated benefits/activities because of one of the enumerated characteristics.

#### **D. 18 U.S.C. § 247: Damage to Religious Property; Obstruction of Persons in the Free Exercise of Religious Beliefs**

*Islamberg, located in upstate New York, is home to a small African-American Muslim community that had been the subject of online conspiracies depicting the community as terrorists. In response to what he read online, Robert Doggart developed a detailed plan to drive to New York, blow up buildings, and kill members of the community. He needed more people to execute his plan, however, so between February and April 2015 he began recruiting people online, in phone calls, and in person. One of the people he tried to recruit was a confidential informant of the FBI. After several phone calls with the informant, the FBI secured a wiretap to monitor Doggart's calls. Doggart's calls included talk of blowing up and burning down the mosque, school, and cafeteria in Islamberg, as well as killing children in the community. Doggart repeatedly spoke about the bombing of the Islamberg mosque as a flashpoint for a civil insurrection. Doggart met with several people he was recruiting, during which time he showed satellite images of the community and described his plan of attack and escape. Doggart was arrested before he could attempt to carry out his plan.*

*In February 2017, Doggart was found guilty of soliciting people to burn down the mosque because of its religious character. He was sentenced to 19 years' imprisonment. At sentencing, the court found that Doggart's conduct was an act of terrorism because it was meant to influence or affect government conduct through intimidation and coercion.<sup>79</sup>*

---

<sup>78</sup> *Id.*

<sup>79</sup> See Department of Justice, Office of Public Affairs, *Chattanooga Man Sentenced for Solicitation to Burn Down a Mosque in Islamberg, New York*, June 15, 2017, <https://www.justice.gov/opa/pr/chattanooga-man-sentenced-solicitation-burn-down-mosque-islamberg-new-york>; *United States v. Doggart*, No. 1:15-CR-39, 2017 WL 2416920, at 9 (E.D. Tenn. June 2, 2017) (concluding, post-trial, that sufficient evidence existed to sustain the defendant's convictions for solicitation to commit a civil rights violation under 18 U.S.C. § 247(a)(1) and solicitation to commit arson of a building under 18 U.S.C. § 844(i), but finding insufficient evidence for convicting the defendant of making threats in interstate commerce).

## 1. Overview

Section 247<sup>80</sup> criminalizes damaging religious real property or obstructing persons in the free exercise of religious beliefs. If a defendant damages religious real property because of the religious nature of the property or obstructs a person's religious exercise, then the government need not establish a bias-motivation for the offense. It must show, however, that the offense was in or affecting interstate or foreign commerce. If the defendant damages religious real property because of the race, color, or ethnic characteristics of anyone associated with the property, then the government need not establish that the offense was connected to interstate or foreign commerce.

### a. Elements

There are three ways of violating § 247. Subsection (a)(1)<sup>81</sup> criminalizes intentionally defacing, damaging, or destroying religious real property, or attempting to do so, because of the religious character of that property. Subsection (a)(2)<sup>82</sup> criminalizes obstructing, by force or threat of force, any person in the enjoyment of that person's free exercise of religious beliefs, or attempting to do so. Subsection (c)<sup>83</sup> criminalizes intentionally defacing, damaging, or destroying religious real property, or attempting to do so, "because of the race, color, or ethnic characteristics of any individual associated with that religious property."<sup>84</sup>

### b. Section 247(a)(1)

To obtain a conviction for violating § 247(a)(1), the government must prove beyond a reasonable doubt that: (1) the defendant defaced, damaged, or destroyed religious real property, or attempted to do so; (2) the defendant acted intentionally; (3) the defendant did so because of the religious character of the property; and, (4) the offense was in or affected interstate commerce or foreign commerce.<sup>85</sup>

"Religious real property" is defined by statute to mean "any church, synagogue, mosque, religious cemetery, or other religious real property, including fixtures or religious objects contained within a place of religious worship."<sup>86</sup> This term was intended to cover "solemn symbols or objects, such as a Torah."<sup>87</sup> In addition, the term "fixtures" is defined as "personal property that is attached to a land or building and that is regarded as an irremovable part of the real property."<sup>88</sup>

To satisfy § 247(a)(1), the defendant must have acted as he did because the property was religious property. "Conviction under [§ 247(a)(1)] requires the prosecutor to show that a defendant intentionally attempted or committed the act of destruction and was motivated to do so by the religious character of the property."<sup>89</sup>

If the defendant acted because of the religious characteristic of the property, the government must prove that the offense was in or affecting interstate commerce.<sup>90</sup> Commerce includes trade, travel, transportation, and communication. The issue of whether an activity takes place in interstate or foreign

---

<sup>80</sup> § 247.

<sup>81</sup> § 247(a)(1).

<sup>82</sup> § 247(a)(2).

<sup>83</sup> § 247(c).

<sup>84</sup> *Ibid.*

<sup>85</sup> § 247(a)(1).

<sup>86</sup> § 247(f).

<sup>87</sup> Statement of Sen. Kennedy on S.1890, 142 CONG. REC. S6517-04, S6522.

<sup>88</sup> *Fixtures*, BLACK'S LAW DICTIONARY (10th ed. 2014).

<sup>89</sup> S. REP. NO. 100-324, 100th CONG., 2d Sess. 1988, *reprinted* in 1988 U.S.C.C.A.N. 721, 723.

<sup>90</sup> *See* § 247(b).

commerce or affects interstate or foreign commerce must be submitted to the jury. The evidence need not show, however, that the defendant knew or intended any effect on interstate commerce.<sup>91</sup>

The constitutionality of § 247(a)(1) has been upheld over Commerce Clause-based challenges.<sup>92</sup> The attached appendix provides a circuit-by-circuit summary of § 247(a)(1) cases issued to date.

### **c. Section 247(a)(2)**

To obtain a conviction for violating § 247(a)(2), the government must prove beyond a reasonable doubt that: (1) the defendant obstructed, by force or threat of force, any person in the enjoyment of that person's free exercise of religious beliefs, or attempted to do so; (2) the defendant acted intentionally; and, (3) the offense was in or affected interstate or foreign commerce.<sup>93</sup>

Both threats and the actual use of physical force against worshippers can satisfy this subsection. Thus, it may be a good option to use in a case involving religious-based threats that cannot be prosecuted under § 249,<sup>94</sup> which lacks a threats provision. As with § 247(a)(1), the government must prove that the offense was in or affecting interstate or foreign commerce. In *United States v. Roof*,<sup>95</sup> the district court upheld the constitutionality of § 247(a)(2) as a valid exercise of Congress's power to enact legislation pursuant to its Commerce Clause authority. The attached appendix provides a circuit-by-circuit summary of § 247(a)(2) cases issued to date.

### **d. Section 247(c)**

To obtain a conviction for violating § 247(c), the government must prove beyond a reasonable doubt that: (1) the defendant defaced, damaged, or destroyed religious real property, or attempted to do so; (2) the defendant acted intentionally; and, (3) the defendant acted because of the race, color, or ethnic characteristics of any individual associated with that religious property.<sup>96</sup>

The term "religious real property" should be given the same meaning as in subsection (a)(1), discussed above. Because Congress did not rely upon its Commerce Clause authority to pass § 247(c), prosecutors need not prove a connection to interstate or foreign commerce. They must, however, prove that the defendant was motivated not because of the religion of the house of worship but by the race or ethnicity of someone associated with it. This provision is thus often used when churches serving an African-American congregation are burned because they are viewed as African-American churches.

As explained above, Congress may prohibit conduct targeting Jews and Arabs through "racial" legislation because such groups were considered a racial group at the time the Thirteenth Amendment was ratified.<sup>97</sup> Section 247 may thus be used, without regard to whether the offense had a connection to interstate or foreign commerce, if the offense was motivated by the fact that worshippers were Jewish or

---

<sup>91</sup> See *United States v. Grassie*, 237 F.3d 1199, 1206 n.5 (10th Cir. 2001); 10th Cir. Crim. Jury Instr. § 2.71 (explaining that, in Hobbs Act prosecution, it is not necessary for government to prove that the defendant knew his conduct would interfere with or affect interstate commerce).

<sup>92</sup> *United States v. Ballinger*, 395 F.3d 1218, 1230 (11th Cir. 2005) (en banc) (holding that "Congress' commerce authority includes the power to punish a church arsonist who uses the channels and instrumentalities of interstate commerce to commit his offenses"); *Grassie*, 237 F.3d at 1211 ("[B]y making interstate commerce an element of the crime under [§ 247], to be decided on a case-by-case basis, constitutional problems are avoided.").

<sup>93</sup> § 247(a)(2).

<sup>94</sup> § 249.

<sup>95</sup> *Roof*, 225 F. Supp. 3d 438, 452-56 (D.S.C. 2016).

<sup>96</sup> § 247(c).

<sup>97</sup> See *Shaare Tefila Congregation v. Cobb*, 481 U.S. 615, 617 (1987) (holding Jews are a race for purposes of 42 U.S.C. § 1982); *Saint Francis College v. Al-Khazraji*, 481 U.S. 604, 613 (1987) (holding Arabs are a race for purposes of 42 U.S.C. § 1981).

Arab. Although not set forth expressly in its legislative findings when Congress enacted § 247 (as Congress would do when it passed § 249), there is nonetheless persuasive evidence that Congress, acting in 1996, meant to adopt the Civil War-era understanding of races. Congressman Hyde described the holdings in *Shaare Tefila* and *Saint Francis College* and then stated that these two cases established that “in passing legislation to protect churches and houses of worship under its [Thirteenth Amendment] authority, Congress may reach attacks not only on churches owned by African-Americans, but churches owned or used by other minority groups, and synagogues as well. Congress’s exercise of its authority to eliminate the badges and incidents of slavery easily supports legislation to make it a crime to deface, damage or destroy a house of worship because of the race, color, or ethnic origin of the person or persons who own or use the building.”<sup>98</sup> The attached appendix provides a circuit-by-circuit summary of § 247(c) cases issued to date.

## II. Using the Civil Rights Conspiracy Statute in Hate Crime Cases

*In the summer of 2000, three people—a Latina woman, a Latino man, and an African-American man—were socializing in a local park in Montana when they were surrounded by nine members of a white supremacist group who were brandishing weapons and “patrolling” the park for racial minorities and Jews. The group, known as the Montana Front Working Class Skinheads, formed earlier that year “to rid the world of all scum, including racial minorities and Jews, using whatever means it took, including violence.” They wore specialized uniforms, shaved their heads, listened to hate music, read racist literature, exhibited tattoos with racist symbols, and were armed at all times. They also recruited minors into the group because minors “were less likely than adults to go to prison for committing violent acts.” Members of the group earned “status” by physically beating up or harming their victims. To this end, members of the group entered the Montana park from different entrances and moved toward the park’s center to “clean out all the minorities.” They encountered the three victims sitting at a picnic table and chased them out of the park while yelling racial slurs. The next day, the leaders of the group berated those involved in the “park patrol” for not chasing, catching, and beating one of the men. The defendants were charged not only with substantive civil rights offenses but also with conspiring to injure, oppress, threaten, and intimidate African-American, Hispanic, Jewish, and Native American persons in the free exercise of their right to enjoy a public accommodation without discrimination. All of the defendants were convicted of violating 18 U.S.C. § 241—the civil rights conspiracy statute. They were sentenced to between 41 and 180 months’ imprisonment.<sup>99</sup>*

The civil rights conspiracy statute under which the defendants were convicted is unique. Enacted over a century ago in response to acts of racial violence committed by the Ku Klux Klan, the statute today remains a powerful tool in the government’s efforts to combat racially-motivated crimes of violence. The conspiracy statute, however, reaches well beyond bias-motivated crimes. In fact, unlike the substantive hate crime statutes discussed in this article, it does not prohibit crimes against individuals based on their protected characteristics (e.g., race or gender), nor does it require the government to establish that a defendant acted with a particular bias motivation. And unlike the general conspiracy statute codified at 18 U.S.C. § 371,<sup>100</sup> it does not prohibit conspiracies to violate criminal statutes. The statute instead prohibits conspiracies designed to violate rights guaranteed by the Constitution or other federal laws—such as occupying a dwelling, enjoying public accommodations, traveling, and attending school. The statute is

---

<sup>98</sup> 142 CONG. REC. H6451-01 at H6453.

<sup>99</sup> See *United States v. Allen*, 341 F.3d 870 (9th Cir. 2003).

<sup>100</sup> 18 U.S.C. § 371 (2012).

also used to prosecute cases involving official misconduct and human trafficking. This article, however, addresses the statute’s scope, history, and elements as they relate to prosecutions of federal hate crimes

Section 241<sup>101</sup> traces its lineage back to the post-Civil War era. In the years immediately following the Civil War, “there was much agitated criticism in the Congress and in the Nation because of the continued denial of rights to [African Americans], sometimes accompanied by violent assaults.”<sup>102</sup> The response over the next five years was swift: the states ratified the Thirteenth Amendment (1865);<sup>103</sup> Congress enacted the Civil Rights Act of 1866,<sup>104</sup> which prohibited violations of rights under color of law—the precursor to present-day 18 U.S.C. § 242,<sup>105</sup> Congress proposed (1866) and the states ratified (1868) the Fourteenth Amendment;<sup>106</sup> and, Congress proposed (1869) and the states ratified (1870) the Fifteenth Amendment.<sup>107</sup> Just a few months after the Fifteenth Amendment was ratified, Congress enacted the Enforcement Act of 1870,<sup>108</sup> which contained the precursor to present-day 18 U.S.C. § 241. Due to narrow legal interpretations, it was little used for many years.

It was not until nearly one hundred years after its original enactment that the Supreme Court expressly ruled that “the purpose and effect” of the Enforcement Act, now codified with modifications at 18 U.S.C. § 241, “was to reach assaults upon rights under the entire Constitution, including the Thirteenth, Fourteenth and Fifteenth Amendments.”<sup>109</sup> A few years later, the Supreme Court declared that “18 U.S.C. § 241 . . . reaches wholly private conspiracies.”<sup>110</sup> If the right at issue, however, is secured by the Fourteenth Amendment, which guarantees rights free from state interference, then the protected right will fall within § 241’s reach only when state action is alleged as part of the conspiracy.<sup>111</sup> For those rights that may be violated without state action, “a purely private conspiracy can suffice for liability” under § 241.<sup>112</sup>

A violation of § 241 always constitutes a felony offense, even when the related substantive actions that defendants conspired to commit would, if executed, only constitute a misdemeanor offense. A conviction under § 241 carries a potential ten-year term of imprisonment. If death results from the conspiracy, or if a defendant’s actions in connection with the conspiracy include kidnapping or aggravated sexual abuse, or attempts at kidnapping, aggravated sexual abuse, or murder, then a defendant may be sentenced to “any term of years or for life, or both, or . . . death.”<sup>113</sup> The statute of limitations for violations of § 241 is five years; if death results from the conspiracy, however, then there is no statute of limitations.<sup>114</sup>

To establish a conspiracy under 18 U.S.C. § 241, the government must prove beyond a reasonable doubt that (1) a conspiracy existed which the defendant joined; (2) the object of the conspiracy was to “injure, oppress, threaten or intimidate” a person or persons in the free exercise or enjoyment of a right

---

<sup>101</sup> 18 U.S.C. § 241(2012).

<sup>102</sup> *United States v. Price*, 383 U.S. 787, 802 (1966).

<sup>103</sup> U.S. CONST. amend. XIII.

<sup>104</sup> Civil Rights Act of Apr. 9, 1866, c. 31, 14 Stat. 27.

<sup>105</sup> § 242.

<sup>106</sup> U.S. CONST. amend. XIV.

<sup>107</sup> U.S. CONST. amend. XV.

<sup>108</sup> Enforcement Act of 1870 (Cong. Globe, 41st Cong., 2d Sess., pp. 3611-3613).

<sup>109</sup> *United States v. Price*, 383 U.S. 787, 805 (1966); *see also* *United States v. Guest*, 383 U.S. 745, 753-57 (1966).

<sup>110</sup> *Griffin v. Breckenridge*, 403 U.S. 88, 104 (1971) (collecting cases).

<sup>111</sup> *See, e.g., United States v. Tarpley*, 945 F.2d 806, 808 n.2 (5th Cir. 1991) (“Although [§ 241] does not contain the words ‘under color of law,’ proof of state action is necessary whenever it is an essential element of a constitutional violation.”).

<sup>112</sup> *United States v. Reese*, 2 F.3d 870, 896 (9th Cir. 1993).

<sup>113</sup> § 241.

<sup>114</sup> 18 U.S.C. §§ 3281 and 3282 (2012).

protected by the Constitution or other federal laws; and, (3) the planned interference with the protected right or rights was willful.<sup>115</sup>

Similar to the general conspiracy statute codified at 18 U.S.C. § 371, § 241 requires the government to prove that the defendants conspired or agreed to commit an unlawful act.<sup>116</sup> Unlike most conspiracies charged under § 371, however, the civil rights conspiracy statute does not require the government to prove an overt act.<sup>117</sup> Moreover, the “unlawful act” must be a violation of the Constitution or of federal law establishing a civil right or privilege, not a violation of criminal law.<sup>118</sup>

The purpose of a conspiracy charged under § 241 must be to injure, oppress, threaten, or intimidate another person in that person’s free exercise or enjoyment of any right or privilege guaranteed by the Constitution or federal law. As at least one court has noted, the words “injure,” “oppress,” “threaten,” or “intimidate” “are not used in any technical sense.”<sup>119</sup> But where the defendant’s challenged conduct is a form of speech or expression, an alleged “threat” to one’s enjoyment or exercise of a right must constitute “a threat of force or the intimidation of physical fear.”<sup>120</sup> Otherwise, the court explained, the statute would run counter to the First Amendment’s protections for speech and/or expressive conduct that, while forceful and offensive, “merely mak[es] someone hesitate before acting in a certain way.”<sup>121</sup> The court further explained that the First Amendment is not implicated when a jury is instructed that the defendant’s actions were intended to “prevent the free action of other persons.”<sup>122</sup> This ruling was informed by the court’s earlier decision overturning on First Amendment grounds the § 241 conviction of a defendant who burned a cross near the apartment building of a minority family. In that case, the court held that the jury was improperly instructed that to “threaten” and to “intimidate” could include “a variety of conduct intended to harm, frighten, punish, or inhibit the free action of other persons,” but that it did not require “a threat of physical force or the intimidation of physical fear.”<sup>123</sup>

Section 241 thus prohibits conspiracies to “threaten” or “intimidate” others in the enjoyment or exercise of their federally protected rights provided the defendant’s actions constitute a “true threat.” As explained above, true threats include statements or actions “where the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence to a particular individual or group of individuals.”<sup>124</sup> “Intimidation,” the Supreme Court reasoned, “is a type of true threat” when made “with the intent of placing the victim in fear of bodily harm or death,” even when the speaker has no intention to carry out the threat.<sup>125</sup> For this reason, when a defendant’s challenged conduct primarily involves speech

---

<sup>115</sup> *United States v. Epley*, 52 F.3d 571, 575-76 (6th Cir. 1995) (“To obtain a conviction for conspiracy to violate civil rights under § 241, the government must prove that [the defendant] knowingly agreed with another person to injure [the victim] in the exercise of a right guaranteed under the Constitution.”).

<sup>116</sup> *See, e.g., United States v. Wander*, 601 F.2d 1251, 1259 (3rd Cir. 1979) (“[T]he gist of [§ 371] is the agreement and specific intent to commit an unlawful act, and when required by statute, an overt act.”).

<sup>117</sup> *See United States v. Colvin*, 353 F.3d 569, 576 (7th Cir. 2003) (en banc) (stating that “§ 241 does not specify an overt-act requirement”); *United States v. Whitney*, 229 F.3d 1296, 1301 (10th Cir. 2000) (same); *United States v. Crochiere*, 129 F.3d 233, 237 (1st Cir. 1997) (stating that “[t]he Supreme Court case of *United States v. Shabani*, 513 U.S. 10 (1994) . . . requires a holding that § 241 contains no overt act requirement”); *United States v. Skillman*, 922 F.2d 1370, 1375-76 (9th Cir. 1990) (stating that § 241 does not require proof of an overt act in furtherance of the conspiracy); *United States v. Morado*, 454 F.2d 167, 169 (5th Cir. 1972) (same); *Wilkins v. United States*, 376 F.2d 552, 562 (5th Cir. 1967) (same).

<sup>118</sup> *United States v. Kozminski*, 487 U.S. 931, 940 (1988).

<sup>119</sup> *United States v. McDermott*, 29 F.3d 404, 408 (8th Cir. 1994).

<sup>120</sup> *Id.* at 408-09.

<sup>121</sup> *Id.* at 409.

<sup>122</sup> *Ibid.*

<sup>123</sup> *United States v. Lee*, 6 F.3d 1297, 1300 (8th Cir. 1993) (en banc).

<sup>124</sup> *Virginia v. Black*, 538 U.S. 343, 359 (2003).

<sup>125</sup> *Id.* at 360.

or expression, it is often necessary to instruct a jury that, for purposes of establishing a § 241 conspiracy, an alleged “threat” against a person’s engagement in a federally-protected right requires a “threat of force.”<sup>126</sup> The Tenth Circuit explained that a threat of force is required to fall within § 241’s prohibitions because “[m]any acts short of unlawful violence may constitute oppression or intimidation in the everyday sense of the words.”<sup>127</sup>

To be sure, not all prosecutions under § 241 require the government to prove a threat of *physical* force. In *United States v. Kozminski*, defendants were charged with willfully conspiring to deprive two victims of their right to be free from involuntary servitude—a right secured by the Thirteenth Amendment.<sup>128</sup> The Court asserted that the Thirteenth Amendment prohibits involuntary servitude “enforced by the use or threatened use of physical *or legal coercion*.”<sup>129</sup> Outside of the unique human trafficking context, where actions to compel someone’s labor may not always incorporate threats of physical force, the government must usually show in § 241 prosecutions that any “threat” by the defendant to interfere with a person’s federally-protected rights involved a threat of force or threat of unlawful violence.<sup>130</sup>

The individual rights that most commonly give rise to § 241 prosecutions generally involve rights associated with (1) housing and property ownership,<sup>131</sup> (2) use of public accommodations,<sup>132</sup> (3) public schooling free of racial discrimination,<sup>133</sup> (4) the right to travel,<sup>134</sup> (5) the right to vote,<sup>135</sup> and (6) the right to inform federal officials about federal crimes,<sup>136</sup> and be a witness in federal cases.<sup>137</sup>

### **III. Using the Hate Crime Sentencing Guidelines to Obtain Greater Penalties in Any Criminal Case with Hate Crime Motivation**

*At a United States Penitentiary in Louisiana, three white inmates, at least one of whom was a suspected member of a white supremacist gang known as the Dirty White Boys, attacked two African-American inmates with ten- to twelve-inch prison-made knives. During the assault, one of the attackers yelled, “Get their eyes,” while all attackers shouted*

---

<sup>126</sup> *United States v. Magleby*, 420 F.3d 1136, 1143 (10th Cir. 2005) (finding fault with jury instructions but finding no ineffective assistance on part of appellate counsel who failed to challenge instructions).

<sup>127</sup> *Ibid.*

<sup>128</sup> *United States v. Kozminski*, 487 U.S. 931, 939-40 (1988).

<sup>129</sup> *Id.* at 944 (emphasis added).

<sup>130</sup> *See, e.g.*, *Magleby*, 420 F.3d at 1143; *Lee*, 6 F.3d at 1300; cf. *Watts v. United States*, 394 U.S. 705, 707-08 (1969) (true threats are not constitutionally protected speech); *Planned Parenthood v. American Coalition of Life Activists*, 290 F.3d 1058, 1077 (9th Cir. 2002) (en banc) (holding that in statute protecting access to clinics, a “threat of force” is “a statement which, in the entire context and under all the circumstances, a reasonable person would foresee would be interpreted by those to whom the statement is communicated as a serious expression of intent to inflict bodily harm upon that person,” otherwise statement is protected by First Amendment).

<sup>131</sup> *See, e.g.*, *United States v. Skillman*, 922 F.2d 1370, 1372 (9th Cir. 1990) (interference with housing rights).

<sup>132</sup> *See, e.g.*, *United States v. Johnson*, 390 U.S. 563, 565-66 (1968) (patronizing a restaurant); *United States v. Allen*, 341 F.3d 870, 876-78 (9th Cir. 2003) (using a public park); *United States v. Baird*, 85 F.3d 450, 452-55 (9th Cir. 1996) (frequenting a convenience store).

<sup>133</sup> *See, e.g.*, *Hayes v. United States*, 464 F.2d 1252, 1261 (5th Cir. 1972) (“[T]he right of black students to attend public schools without regard to race or color is secured by federal statute,” i.e., 42 U.S.C. § 2000c et seq., and therefore a private conspiracy to deprive students of this right is “an offense against the United States.”).

<sup>134</sup> *See, e.g.*, *United States v. Guest*, 383 U.S. 745, 759 n.17 (1966) (“[T]he constitutional right of interstate travel is a right secured against interference from any source whatever, whether governmental or private.”).

<sup>135</sup> *See, e.g.*, *United States v. Classic*, 313 U.S. 299, 315 (1941) (federal primary elections); *Ex parte Yarbrough*, 110 U.S. 651 (1884) (federal elections).

<sup>136</sup> *See, e.g.*, *Motes v. United States*, 178 U.S. 458, 462-63 (1900) (right to inform about a federal crime).

<sup>137</sup> *See, e.g.*, *United States v. DiNome*, 954 F.2d 839, 845 (2d Cir. 1992) (federal witness).

*racial slurs. One of the victims lost vision in one eye; the other suffered puncture wounds to his head, neck, face, and arms.*

*The attackers were charged with two counts of assault with a deadly weapon, in violation of 18 U.S.C. § 113(a)(3)—one count for each victim. One of the attackers pled guilty to one of the counts and was sentenced to 100 months in prison. During sentencing, the district court added a three-level upward adjustment pursuant to U.S.S.G. § 3A1.1(a) when calculating the defendant’s offense level because the defendant selected his victims based on race. In upholding the adjustment, the court of appeals concluded that the evidence presented at the defendant’s sentencing hearing established beyond a reasonable doubt that, among other things, the attackers shouted racial epithets during the attack and the defendant knew the attack was planned for retaliatory reasons against African-American inmates.<sup>138</sup>*

Since 1995, the Federal Sentencing Guidelines (Guidelines) have provided for sentencing adjustments when a defendant specifically targets a victim based upon a victim’s personal characteristic, such as race or gender.<sup>139</sup> These adjustments are most often applied when a defendant is convicted of violating one of the federal hate crime statutes. These adjustments may also be used, however, when a defendant is convicted of a general federal criminal offense but the evidence supports a finding that the defendant selected his victim because of a particular characteristic of the victim, as set forth in the example above. In effect, application of the adjustment in these circumstances results in a hate crime sentence for a conviction of a non-hate crime offense.

The Guidelines provide for a three-level upward adjustment to a defendant’s base offense level if the defendant “intentionally selected any victim or any property as the object of the offense . . . because of the actual or perceived race, color, religion, national origin, ethnicity, gender, gender identity, disability, or sexual orientation of any person.”<sup>140</sup> Gender identity was added in 2010, following passage of the Shepard-Byrd Act. Because § 3A1.1(a) includes both gender identity and sexual orientation as bases for adjusting upward a defendant’s offense level, § 3A1.1(a) has a broader reach than both the criminal provision of the Fair Housing Act, 42 U.S.C. § 3631,<sup>141</sup> and the protections against interference with federally-protected rights set forth in 18 U.S.C. § 245(b),<sup>142</sup> as neither of these statutes criminalizes actions taken because of the actual or perceived gender identity or sexual orientation of the victim. Moreover, if a prosecutor can prove a violation of any existing non-hate criminal statute, and can also prove that the defendant acted with a hate crime motivation, the prosecutor can effectively transform a violation of a traditional criminal statute into a hate crime conviction by seeking the accompanying enhanced penalty associated with hate crimes.

Doing so requires planning, however, as the hate crime adjustment, unique among all other guidelines, requires the finder of fact at trial, or a court at sentencing in the case of a plea, to determine beyond a reasonable doubt that the defendant intentionally selected the victim (or property) because of the actual or perceived characteristic of the victim (or property). This requirement is easily satisfied when the defendant has been convicted after trial or pleaded guilty to a traditional federal hate crime offense, discussed *infra*, which includes as an element of the offense proof that the defendant acted because of a particular characteristic of the victim.<sup>143</sup> In such a case, no special verdict form need be submitted to the

<sup>138</sup> See *United States v. Horsting*, 204 Fed. App’x 441 (5th Cir. 2006).

<sup>139</sup> U.S. SENTENCING GUIDELINES MANUAL § 3A1.1(A) (U.S. SENTENCING COMM’N. 2016) (hereinafter U.S.S.G.).

<sup>140</sup> U.S.S.G. § 3A1.1(a).

<sup>141</sup> § 3631.

<sup>142</sup> § 245(b).

<sup>143</sup> See, e.g., § 245(b)(2) (criminalizing conduct where the defendant has acted “because of” the victim’s “race, color, religion, or national origin” and because the victim was engaged in a federally-protected activity); § 247(b) (criminalizing conduct where the defendant destroys religious real property “because of the race, color, or ethnic

jury as the bias motivation will have been submitted to them as part of the underlying crime upon which it must render its verdict.<sup>144</sup>

For commonly charged offenses that do not have as an element of the offense proof that the defendant acted because of a protected characteristic of the victim, but where the evidence nonetheless establishes beyond a reasonable doubt that the defendant was so motivated, the adjustment may still apply. For example, the civil rights conspiracy statute, set forth at 18 U.S.C. § 241,<sup>145</sup> is frequently charged in hate crime prosecutions, but it does not require the government to establish that a defendant acted pursuant to a bias motivation. As the Sixth Circuit explained, “§ 241 does not assume that a victim of a civil rights conspiracy will be a member of a [protected] group” and could instead “involve a conspiracy to deny interstate travel or the right to procedural due process.”<sup>146</sup> But, where the facts support charging a civil rights conspiracy (or other offense without a bias motivation element) and the government proves beyond a reasonable doubt that the defendant acted with a bias motivation, application of the hate crime motivation adjustment is warranted.<sup>147</sup>

In such cases, prosecutors may use special verdict forms for the jury to determine expressly whether the evidence presented at trial established beyond a reasonable doubt the defendant’s motivation. At least one court, however, has held that a special verdict form is not required where the nature of the conviction itself supports such a finding. In *In re Terrorist Bombings of U.S. Embassies in East Africa*,<sup>148</sup> the court of appeals upheld the district court’s application of the hate crime motivation adjustment for a defendant convicted of multiple offenses arising from his and others’ involvement in the bombings of two American embassies in Africa. Although the jury was not expressly asked to determine the defendants’ motivations, all defendants were convicted of, among other offenses, conspiring to murder U.S. nationals in violation of 18 U.S.C. § 2332(b).<sup>149</sup> The court of appeals rejected the argument that the defendants

---

characteristics” of anyone associated with the property); § 249 (criminalizing conduct where the defendant causes bodily injury to any person because of the victim’s actual or perceived race, color, religion, national origin, gender, sexual orientation, gender identity, or disability); § 3631 (criminalizing conduct where the defendant interferes with a person’s housing rights because of the person’s race, color, religion, sex, disability, or national origin); *but see* § 241 (criminalizing conspiracies to violate civil rights without regard to any protected characteristic of the victim).<sup>144</sup> Applying the § 3A1.1 adjustment when a defendant has been convicted of a hate crime that has as an element of the offense proof that the defendant selected his or her victim because of a victim’s protected characteristic does not result in impermissible double counting when calculating a defendant’s offense level for sentencing purposes. The commentary to the Guidelines expressly states that the hate crime motivation adjustment “applies to hate crimes.” U.S.S.G. § 3A1.1, Application Note 1. Moreover, courts have rejected arguments that applying the adjustment when calculating offense levels for hate crime convictions constitutes impermissible “double counting.” *See, e.g.,* United States v. Endsley, No. 08-40050-01-SAC, 2009 WL 385864 (D. Kan. Feb. 17, 2009) (applying the adjustment when sentencing defendant who pleaded guilty to a misdemeanor offense of 42 U.S.C. § 3631 and rejecting argument that doing so resulted in “double counting” because the guideline applicable to defendant’s offense, U.S.S.G. § 2H1.1, “expressly allows for a hate crime enhancement under U.S.S.G. § 3A1.1(a)”). In a recent case seemingly in direct contradiction to the plain language of the Guidelines and applicable case law, however, a sentencing court refused to apply the three-level adjustment set forth at § 3A1.1(a) where the defendant pleaded guilty to violating

§ 245(b)(2)(A) after he draped a confederate flag and hung a noose on the statue of James Meredith on the campus of the University of Mississippi. United States v. Harris, 128 F. Supp. 3d 957 (D. Miss. 2015). The court reasoned that the underlying offense of conviction already took into consideration the race of the victim and therefore applying the adjustment would be impermissibly duplicative. *Id.* at 962.

<sup>145</sup> § 241.

<sup>146</sup> United States v. Salyer, 893 F.2d 113, 115-16 (6th Cir. 1989).

<sup>147</sup> *See, e.g.,* United States v. Weems, 517 F.3d 1027 (8th Cir. 2008) (court of appeals reversed district court that refused to apply three-level adjustment after defendant was convicted of conspiracy, in violation of § 241, after he and others burned a cross outside the home of an African-American man).

<sup>148</sup> *In re Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 93 (2d Cir. 2008).

<sup>149</sup> *Id.* at 107.

targeted victims based upon their citizenship rather than their national origin, holding that such an argument ran counter to the jury’s verdict that the defendants “conspired to murder nationals of the United States,” and that because the adjustment applies to actual or perceived national origin, “it was not necessary for al Qaeda to distinguish between nationals and citizens, or naturalized and birthright U.S. citizens, so long as it perceived the victims as having a U.S. national origin.”<sup>150</sup>

A district court relied on the holding in *In re Terrorist Bombings* to hold expressly that “no special verdict is required to impose [the hate crime] enhancement.”<sup>151</sup> The district court in that case applied the hate crime motivation adjustment when sentencing the defendant for his various convictions arising from planning and attempting to carry out domestic terrorism offenses involving a plot to bomb two synagogues.<sup>152</sup> The district court reasoned that because the jury “necessarily found that the defendants deliberately decided to attack those specific places, the jury’s verdict necessarily implies that the victims were selected for attack because of their religion.”<sup>153</sup> Quoting *In re Terrorist Bombings*, the district court reasoned that “‘it is the very fact that [the defendants were] convicted of these offenses that justifies the application of the hate crime . . . enhancement.’”<sup>154</sup> Still, if a prosecutor wants to rely on the adjustment at sentencing, he or she may wish to submit a special verdict form to the jury so that there is no question whether the finder of fact has found sufficient evidence of a hate crime motivation, particularly if the motivation is a disputed issue at trial.

Where a defendant pleads guilty to a non-hate crime offense, but where the facts of the case indicate beyond a reasonable doubt that the defendant was motivated by a protected characteristic of the victim, the adjustment also may be used. If appropriate, the government should include a defendant’s motivation in his plea agreement to support the application of the hate crime motivation adjustment at sentencing. In other cases, the sentencing court may rely on factual findings set forth in the presentence report to support the application of the adjustment, provided those facts are established beyond a reasonable doubt. In either case, the government should ensure that the court uses the “beyond a reasonable doubt” standard when making its determination in the absence of jury findings. For example, a defendant pleaded guilty to, among other charges, two counts of making threatening communications in violation of 18 U.S.C. § 875,<sup>155</sup> after he emailed communications containing death threats and ethnic slurs to two individuals.<sup>156</sup> In calculating the defendant’s offense level, the district court applied the three-level hate crime motivation adjustment “based on its finding of facts as set forth in the presentence investigation report.”<sup>157</sup> The presentence report asserted that the defendant’s threatening communications included the “frequent use of ethnic slurs” and the use of a “derogatory term contained in the email address” directed to one of the victims.<sup>158</sup> The report continued that, “it appears the defendant intentionally selected” one of his victims based on what the defendant thought were her religious beliefs.<sup>159</sup> The court explained that, given complainant’s “hate speech,” it found beyond a reasonable

---

<sup>150</sup> *Id.* at 154.

<sup>151</sup> *United States v. Cromitie*, No. 09 CR. 558 CM, 2011 WL 2693293 (S.D.N.Y. June 29, 2011).

<sup>152</sup> *Id.* at 7; *see also* *United States v. Cromitie*, 727 F.3d 194, 199 (2d Cir. 2013) (providing additional facts of the offense).

<sup>153</sup> *Id.*

<sup>154</sup> *Ibid.* (quoting *In re Terrorist Bombings*, 552 F.3d at 153); *see also* *United States v. Hassan*, 2012 WL 147952, 4 n.3 (E.D.N.C. Jan. 18, 2012) (applying the adjustment over the defendant’s objections after concluding that the evidence at trial established beyond a reasonable doubt that, in “conspiring to commit terrorist acts aimed at ‘kuffar,’ or non-Muslims,” in violation of 18 U.S.C. § 2339A, the defendant intentionally selected victims based on religion, national origin, and/or ethnicity).

<sup>155</sup> 18 U.S.C. § 875 (2012).

<sup>156</sup> *Crosby v. United States*, No. 2:11-cr-00023-GZS, 2015 WL 1457430, 1 (D. Me. Mar. 30, 2015).

<sup>157</sup> *Id.* at 9.

<sup>158</sup> *Ibid.*

<sup>159</sup> *Ibid.*

doubt that the defendant intentionally selected his victim based upon his beliefs about her ethnicity or her religious beliefs, and therefore the adjustment applied.<sup>160</sup>

## IV. Non Hate Crime Statutes

Prosecutors should be prepared, as in all cases involving violent crimes, to look for additional, related criminal charges to bring along with federal hate crime charges. Such crimes might include federal firearms charges or charges for lies or obstruction during federal investigations. However, there may be times when, due to the gaps in federal coverage described above, there are no federal hate crimes that apply. In such cases, prosecutors must charge violations of other federal statutes. The federal statutes most commonly used in hate crime prosecutions are described below.

### A. Arson Statutes

Many hate crimes are committed through the use of fire. Arson of homes, places of employment, cars, and other structures is not uncommon in hate crime cases. In addition, because of the long and terrible history of cross-burning by the Klan in the United States, many hate crime defendants, whether or not they are part of an organized hate group, burn crosses as a means of intimidation.

#### 1. Section 844(i)

Section 844(i)<sup>161</sup> criminalizes damaging or destroying by means of fire or an explosive any building, vehicle, or real property used in interstate or foreign commerce. In determining whether arson of a particular building is prosecutable, prosecutors must first determine whether the building was used in interstate or foreign commerce or in an activity affecting interstate or foreign commerce. If it was, prosecutors should consider charging § 844(i). The Supreme Court has held that, in analyzing whether there is a link to interstate or foreign commerce, the “proper inquiry” is into the function of the building itself, and then a determination of whether that function affects interstate commerce.<sup>162</sup>

Under *Jones v United States*, a private residence that does not contain a home-business will almost never qualify as “in or affecting commerce.”<sup>163</sup> Arson of an ongoing, commercial business, on the other hand, will likely qualify.<sup>164</sup> Arson of a rental property is also likely to qualify.<sup>165</sup> For other kinds of buildings, prosecutors will likely have to conduct an in-depth analysis of the function of the building and its ties to commercial activity and examine the law in the relevant circuit.<sup>166</sup>

---

<sup>160</sup> *Ibid.*

<sup>161</sup> 18 U.S.C. § 844(i) (2012).

<sup>162</sup> *Jones v. United States*, 529 U.S. 848, 854-55 (2000).

<sup>163</sup> *See id.* at 850-51 (“[W]e hold that an owner-occupied residence not used for any commercial purpose does not qualify as property ‘used in’ commerce or commerce-affecting activity; arson of such a dwelling, therefore, is not subject to federal prosecution under § 844(i).”).

<sup>164</sup> *Ibid.*

<sup>165</sup> *Id.* at 853.

<sup>166</sup> *See, e.g., United States v. Adame*, 827 F.3d 637, 644 (7th Cir.) (commerce element satisfied by evidence that rental building was used as office space and two residential apartments), cert. denied, 137 S. Ct. 407 (2016); *United States v. Mahon*, 804 F.3d 946, 951 (9th Cir. 2015) (noting that “an intrinsically noneconomic building can qualify under § 844(i) if the building actively engages in interstate commerce or activity that affects interstate commerce, as there is no categorical exclusion of any type of building”).

## 2. Section 844(h)

An arson of a private dwelling which cannot be prosecuted under § 844(i) may be prosecutable under § 844(h)<sup>167</sup> if the arson occurred during the commission of another federal crime, such as a criminal violation of the Fair Housing Act.<sup>168</sup> The federal hate crime statutes discussed above may serve as the predicate offense for a § 844(h)(1) charge.<sup>169</sup> Circuits are split on whether a § 241 conspiracy can serve as the predicate felony for a § 844(h)(1) conviction.<sup>170</sup> In *United States v. Magleby*,<sup>171</sup> the Tenth Circuit expressed doubts about the Seventh Circuit's analysis in *United States v. Colvin*, noting that conspiracy is a continuing offense that encompasses acts performed in furtherance of the agreement. While the Tenth Circuit intimated that it would not likely follow *Colvin*, it sidestepped the issue because it had not been raised on direct appeal.<sup>172</sup>

## B. Interstate Threats: 18 U.S.C. §§ 875 and 876

Section 875(c)<sup>173</sup> makes it a crime to “transmit[] in interstate or foreign commerce any communication containing . . . any threat to injure the person of another.” Section 876<sup>174</sup> makes it a crime to mail threatening communications. Neither of these statutes requires any proof of bias motivation. Provided all the elements are met, however, they may still be charged when the threats at issue are motivated by bias against a protected characteristic or by some other factor, such as personal dislike or extortion. Because § 249<sup>175</sup> does not cover threats and because none of the other federal hate crime statutes, which do cover threats, applies to conduct motivated by LGBT status, §§ 875 and 876 may be a prosecutorial option if interstate threats are made against someone because of his or her sexual orientation or transgender status.

In prosecuting such cases, as in prosecuting any “threats” case, it is important that prosecutors prove that the statement is more than disquieting or upsetting and is, in fact, a “true threat.” As explained above, true threats are “statements where the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence to a particular individual or group of individuals.”<sup>176</sup>

---

<sup>167</sup> § 844(h).

<sup>168</sup> § 3631.

<sup>169</sup> See *United States v. Colvin*, 353 F.3d 569, 575 (7th Cir. 2003); *United States v. Odom*, 252 F.3d 1289, 1292 (11th Cir. 2001) (using § 247 as a predicate felony for a § 844(h)(1) charge); *United States v. Grassie*, 237 F.3d 1199, 1212-16 (10th Cir. 2001) (same).

<sup>170</sup> Compare *United States v. Wildes*, 120 F.3d 468, 469 (4th Cir. 1997) (holding that the conspiracy to violate civil rights by burning a cross could serve as the predicate felony) and *United States v. Stewart*, 65 F.3d 918, 926-28 (11th Cir. 1995) (affirming convictions for §§ 241 and 844(h)(1) and 42 U.S.C. § 3631 as not violating Double Jeopardy Clause) with *Colvin*, 353 F.3d at 575 (holding that § 241 could not serve as the predicate felony because the offense of conspiracy is complete upon agreement) and *United States v. Lee*, 935 F.2d 952, 958 (8th Cir. 1991) (reversing § 844(h)(1) conviction because congressional intent to apply to a cross-burning was unclear).

<sup>171</sup> *United States v. Magleby*, 420 F.3d 1136, 1145-46 (10th Cir. 2005).

<sup>172</sup> *Ibid.*

<sup>173</sup> § 875(c).

<sup>174</sup> 18 U.S.C. § 876 (2012).

<sup>175</sup> § 249.

<sup>176</sup> *Virginia v. Black*, 538 U.S. 343, 359 (2003); *United States v. Dutcher*, 851 F.3d 757, 761 (7th Cir.) (explaining *Virginia v. Black*), cert. denied, No. 16-9610, 2017 WL 2654689 (U.S. Oct. 2, 2017); *United States v. Wheeler*, 776 F.3d 736, 743 (10th Cir. 2015) (explaining *Virginia v. Black*).

## C. Crimes Occurring on Federal Land

Hate crimes which occur on federal land may be prosecuted, not only under hate crime statutes, but also under statutes of general applicability—such as federal murder and assault statutes.<sup>177</sup> Prosecutors trying such cases should be sure to submit the question of the defendant's hate crime motivation to the jury on a special verdict form. Even though it is not necessary to prove bias motivation to convict a defendant on federal murder and assault statutes, as noted above, the Sentencing Guidelines provide that when the trier of fact finds beyond a reasonable doubt that the crime was motivated by bias, the defendant's base offense level will be increased by three levels.<sup>178</sup>

## V. Conclusion

Hate crimes are serious crimes that can tear communities apart. Federal prosecutors should thus be prepared to use every tool available to bring perpetrators to justice. The Criminal Section of the Civil Rights Division stands ready to assist in this endeavor, whether a USAO needs assistance with prosecutions, jury instructions, or for assistance in obtaining the certification required by many of the statutes described above. For questions or assistance, please contact the Civil Rights Division's Criminal Section and ask to speak to the Deputy Chief who supervises the prosecution of hate crimes in your area.

### ABOUT THE AUTHORS

□ **Barbara Kay Bosserman** has served as the Deputy Chief of the Cold Case Unit of the Criminal Section of the Civil Rights Division since April 2017; in this capacity, she works on implementation of the Emmett Till Reauthorization Act. She has served as Senior Legal Counsel of the Criminal Section since October 2008. Prior to the passage of the Matthew Shepard and James Byrd, Jr., Hate Crimes Prevention Act, Ms. Bosserman provided advice and counsel to the Department regarding its position on the pending hate crime legislation. Since the Act's passage, she has worked on developing and implementing training on this Act, as well as on other federal hate crime laws. In 2010, she was part of a team that received the John Marshall Award for work on the Shepard-Byrd Act.

Ms. Bosserman joined the Civil Rights Division in May of 2000. She was detailed to New Orleans, Louisiana, for nine months in 2007, working as an Assistant United States Attorney for the Eastern District of Louisiana. Prior to joining the Department of Justice, Ms. Bosserman worked as a staff attorney for the Fifth Circuit Court of Appeals; as a Legal Services Attorney in Saginaw, Michigan; and as a law clerk in federal district court in the Western District of Michigan. She received her J.D. from The George Washington University in 1991.

□ **Angela M. Miller** joined the Civil Rights Division through the Attorney General's Honors Program in 2002 and is currently detailed to the Division's Criminal Section. She worked for over a decade as a Senior Attorney in the Division's Appellate Section, where she represented the United States in civil rights cases in the United States Courts of Appeals and, in cooperation with the Solicitor General, in the United States Supreme Court. While in the Appellate Section, Ms. Miller focused primarily on handling appeals and providing counsel in criminal matters. In 2010, she was detailed for six months to the Appellate Division of the United States Attorney's Office for the District of Columbia. Before joining the Department of Justice, Ms. Miller clerked on the United States Court of Appeals for the District of Columbia Circuit and served as a behavioral research specialist for the United States Secret Service. She received her J.D., *summa cum laude*, from George Mason University School of Law.

<sup>177</sup> See, e.g., 18 U.S.C. §§ 113 (2012) (assault within maritime and territorial jurisdiction); 1111(b) (2012) (murder within maritime and territorial jurisdiction).

<sup>178</sup> See U.S.S.G. § 3A1.1(a).

Appendix<sup>1</sup>  
Hate Crime Cases By Circuit

**First Circuit**

*United States v. Jacques*, 744 F.3d 804 (1st Cir. 2014)

The court of appeals affirmed convictions for violating 18 U.S.C. § 241, 18 U.S.C. § 247(c), and 18 U.S.C. § 844(h)(1) in connection with an arson of an African-American church. The issues on appeal were unrelated to federal hate crimes.

*United States v. Sharp*, 81 F.3d 147 (1st Cir. 1996) (unpublished)

The defendant was convicted of violating 42 U.S.C. § 3631 for burning a cross near the home of an African-American couple. On appeal, the defendant challenged the application of a two-level sentencing adjustment for his leadership role in the offense. The court upheld the enhancement, noting that the determination of one's role in the offense is "fact-specific and may be based on circumstantial evidence and on a view of the whole of the defendant's pertinent conduct."

*United States v. Page*, 84 F.3d 38 (1st Cir. 1996)

Defendants pled guilty to two counts of violating 18 U.S.C. § 245 after they accosted several Hispanic men attempting to enter a convenience store, called them racial epithets, and made violent threats. As the victims attempted to drive away, the defendants gave chase and fired a gun at their car, injuring one of the victims. On appeal, the court held that although only one victim was wounded, both counts of conviction were subject to the penalty enhancement for bodily injury. "We find nothing in the statutory language to support reading the penalty provision of § 245(b) to permit enhancement only in cases of bodily injury to the intended victim of the particular offense. Nor is there anything indicating an intent to restrict penalty enhancement to a single count when multiple counts aimed at several individuals end up causing but a single bodily injury."

*United States v. Griffin*, 525 F.2d 710 (1st Cir. 1975)

The defendant was convicted of violating 18 U.S.C. § 245(b)(4)(A) for his assault on an African American during a protest against enforced busing in South Boston public schools. The defendant argued on appeal that there was "no direct evidence that by the act of beating [the victim] the defendant intended to prevent black students from attending school." The court held that, given the circumstances, it was for the jury to find that the "defendant intended the indiscriminate beating of an innocent black on the public street near a school . . . to have a chilling effect upon other blacks, parents or children. The general inculcation of fear in order to further a specific objective is a familiar practice." The government was not required to prove that the defendant "knew he was violating a federal statute. It was enough under 18 U.S.C. § 245 that he purposely sought to interfere with the right of black children to go to school; he need not know the exact extent, or the federal character of that right."

*United States v. Three Juveniles*, 886 F. Supp. 934 (D. Mass. 1995)

The defendants, juvenile skinheads who believed that their city had become overrun by black and Jewish residents, and who favored the adoption of abusive tactics in order to scare them into leaving, were convicted of violating 18 U.S.C. § 241 and 18 U.S.C. § 371 (general conspiracy) for conspiring to intimidate local citizens in violation of 18 U.S.C. §§ 245(b)(2)(B) and (F). The court held, with no discussion, that the streets and sidewalks of Brockton were facilities administered by Brockton, a subdivision of the Commonwealth of Massachusetts, within the meaning of § 245(b)(2)(B). The court also held that a mall and its garage were facilities within the meaning of § 245(b)(2)(F) for two reasons. First, the mall held itself out as serving the patrons of all the stores it contained, including eight restaurants, which were facilities under the plain language of § 245(b)(2)(F). Second, the mall sponsored entertainment events, such as home shows, car shows, fashion displays, and Santa Claus exhibitions, and any establishment which presents a performance for the amusement of a viewing public is covered by § 245(b)(2)(F). Moreover, the court held that because the mall was a covered facility by virtue of its presentation of performances, a bookstore was covered by § 245(b)(2)(F) because it held itself out as serving the patrons of the mall and was located within the premises of the mall.

---

<sup>1</sup> These summaries contain abbreviated recitations of the facts and legal decisions and are provided solely as a reference aid. Attorneys intending to cite these cases in court filings should independently confirm the facts and ensure that the holdings remain valid statements of applicable law.

## Second Circuit

*United States v. Nelson*, 277 F.3d 164 (2d Cir. 2002)

The defendants were convicted of violating 18 U.S.C. § 245(b)(2)(B) after they violently beat a Jewish man following a car accident involving a different Jewish man and two African-American children. Although the court of appeals ultimately vacated and remanded because of an error in empaneling the jury, the court upheld the constitutionality of 18 U.S.C. § 245, approved the “streets theory” of prosecution, and held that the second “because of” element in the statute required only an activities-based intent, not motive. The court further approved a jury instruction that permitted the jury to infer, from an attack that occurred on the street, a specific intent to interfere with the victim’s use of the street.

*United States v. Tuffarelli*, 111 F.3d 124 (2d Cir. 1997) (unpublished)

The defendant was convicted of two misdemeanor counts of violating 42 U.S.C. § 3631 after threatening both a white woman in his neighborhood who was considering selling her home to a black couple, and the black couple who had toured the home. On appeal, he argued that the district court erred at sentencing by not grouping the two counts of conviction because the white home seller was only an “indirect or secondary” victim and the main victims were the black home buyers. The court of appeals disagreed, finding that both the black home buyers and the white home seller were equal victims who were both “directly and seriously affected by the defendant’s threats of force.”

*United States v. Anzalone*, 555 F.2d 317 (2d Cir. 1977)

The defendant was convicted of violating 42 U.S.C. § 3631 for shooting out the windows of a black couple’s home, splashing paint on their front door, and attempting to burn down their house. The convictions were reversed because of a violation of *Kastigar v. United States*, 406 U.S. 441 (1972).

*Munger v. United States*, 827 F. Supp. 100 (N.D.N.Y. 1992)

After pleading guilty to one count of violating 42 U.S.C. § 3631 for burning a cross in front of an interracial couple’s home, the defendant argued on appeal that applying the vulnerable victim enhancement when sentencing him was inappropriate. According to the defendant, the victim’s race was a “necessary prerequisite to the commission of his offense,” thereby precluding application of the enhancement. The court disagreed, holding that the underlying guideline did not specifically incorporate race. The court declined to find that “black Americans are per se vulnerable victims” to cross-burnings. Instead, the court found that the victim’s race, his interracial marriage, and the presence of his young daughter in the home all meant that the defendant knew or should have known that his victim was particularly vulnerable.

## Third Circuit

*United States v. Piekarsky*, 687 F.3d 134 (3d Cir. 2012)

The defendants were convicted of violating 42 U.S.C. § 3631 following a fatal beating of an immigrant. The defendants argued the jury instructions were inadequate because they failed to properly instruct on motive. The court of appeals first explained that § 3631(a) criminalizes intimidating or interfering with any person “*because of his race . . . and because he is or has been . . . occupying . . . any dwelling.*” The court rejected the defendant’s contention that the word “because” required proof that the *sole* or *primary* motivation for the assault was race and occupancy, and that the jury should have been instructed accordingly. Relying on decisions of other circuits, the court held that, as long as a § 3631 crime is based *in part* on racial animus, it falls within the scope of the statute. This holding has been partially overturned by *Burrage v. United States*, 134 S. Ct. 881 (2014). The court also held that the statute’s protections applied to *any* person (regardless of immigration status) because of his race, color, or national origin, and that the statute did not require the victim to be a resident (or future resident). Rather, it noted that under § 3631(b) it was sufficient that an individual is victimized “in order to intimidate . . . any other person or any class of persons” from exercising their federally-guaranteed housing rights. Thus, all the government needed to prove at trial was that the victim was injured to send a message to others that they were not welcome in the neighborhood on account of their race, color, or national origin.

*United States v. Stewart*, 806 F.2d 64 (3rd Cir. 1986)

The defendant was convicted of violating 18 U.S.C. § 241 for his role in the arson of a home that was owned by an African American family but unoccupied on the night of the fire. On appeal, the court rejected defendant’s argument that he could not interfere with the owners’ right to occupy their house unless someone was actually exercising his right to occupy the house at the time of the offense. The court held that the evidence showed the defendant was motivated by an

intent to interfere with the owners' rights because he wanted to prevent them from moving back into the house, as well as to prevent other African American families from moving in.

#### **Fourth Circuit**

*United States v. Hill*, No. 16-4299, 2017 WL 3575241 (4th Cir. Aug. 18, 2017)

The court of appeals reviewed the district court's decision that 18 U.S.C. § 249(a)(2) was unconstitutional as applied to a homophobic assault on an Amazon worker who was assaulted while preparing packages for interstate transport. The court did not decide whether the factors were sufficient to support the legislation; instead, it found that the facts had not been sufficiently developed. It stated that the face of the indictment sufficiently laid out a constitutional exercise of Congressional power by alleging that the defendant's conduct had an effect on commerce. It then held that because the defendant raised an as-applied challenge, "whether [the defendant's] conduct sufficiently affects interstate commerce as to satisfy the constitutional limitations placed on Congress' Commerce Clause power may well depend on a consideration of facts, and because the facts proffered here may or may not be developed at trial, it is premature to determine the constitutional issues." It reinstated the indictment and remanded the case.

*United States v. Shifler*, 340 Fed. App'x 846 (4th Cir. 2009) (unpublished)

The defendant pled guilty to violating 18 U.S.C. § 245(b)(2)(A) and 42 U.S.C. § 3631 for interfering with attendance at public schools and with housing rights. The court of appeals' short opinion concluded that the defendant's plea was knowing and voluntary.

*United States v. Hobbs*, 190 Fed. App'x 313 (4th Cir. 2006) (unpublished)

Defendants were convicted of violating 18 U.S.C. § 241 after they conspired to drive an African American family to leave town by shouting racial epithets and throwing trash while driving past the family's home, hanging a noose on their door, leaving a dead animal on their doorstep, and burning a cross in their yard. The appeal raised issues unrelated to the scope or constitutionality of § 241.

*United States v. Nichols*, 149 Fed. App'x 149 (4th Cir. 2005) (unpublished)

The defendant was convicted of two counts of violating 42 U.S.C. § 3631 and one count of 18 U.S.C. § 241 after he and a co-conspirator—deceased at the time of trial—targeted three homes in their neighborhood whose occupants were either Latino or African American. Specifically, they physically assaulted one victim and committed various acts of property destruction, including using steel pipes to smash the windows of a house and a vehicle. On appeal, the court held that sufficient evidence supported the conviction and found that the defendant was not entitled to a misdemeanor instruction.

*United States v. May*, 359 F.3d 683 (4th Cir. 2004)

The defendant was convicted of violating 42 U.S.C. § 3631 for burning a cross to intimidate an interracial couple. The district court granted downward departures at sentencing on the basis of victim conduct, aberrant behavior, and acceptance of responsibility. The court of appeals found all of these departures unwarranted and noted that "even highly provocative behavior does not justify a downward departure if the defendant's response is disproportionate."

*United States v. Crook*, 198 F.3d 238, 1999 WL 957713 (4th Cir. 1999) (unpublished)

The defendant pled guilty to violating 18 U.S.C. § 245(b)(2)(A) after he placed flyers containing racially offensive and violent statements on a number of bulletin boards at a college and in the mail boxes of sixteen African American students at the college. His twelve-month sentence was affirmed on appeal.

*United States v. Smith*, 161 F.3d 5, 1998 WL 633319 (4th Cir. 1998) (unpublished)

Defendants were convicted of violating 18 U.S.C. § 241, 42 U.S.C. § 3631, and 18 U.S.C. § 844(h)(1) after burning a cross at the home of a bi-racial couple. In this short *per curiam* opinion, the court of appeals dismissed defendants' argument that § 844(h)(1) (use of fire to commit a felony) does not apply to underlying conspiracy statutes, such as § 241.

*United States v. Sheldon*, 107 F.3d 868 (4th Cir. 1997) (unpublished)

The defendant appealed his convictions for violating 18 U.S.C. § 241 and 42 U.S.C. § 3631 for building and burning a cross in front of a home occupied by an interracial couple. The defendant argued that his convictions violated his First Amendment rights and that the district court improperly permitted evidence of his racial animus. The court found no First Amendment violation (finding that the instructions were consistent with *Brandenburg v. Ohio*, 395 U.S. 444 (1969)) and

also found no abuse of discretion in the evidentiary rulings. The court held that enhancements in sentencing for both hate crime motivation (§ 3A1.1(a)) and vulnerable victim (§ 3A1.1(b)) were not duplicative because the latter enhancement was based not solely on race but also on the isolated location of the victims' home.

*United States v. Wildes*, 120 F.3d 468 (4th Cir. 1997)

The defendants were convicted of violating 18 U.S.C. § 241, 18 U.S.C. § 844(h), and 42 U.S.C. § 3631(a) for burning a cross in the front yard of an African American family's home. The defendants appealed their § 844(h)(1) conviction on grounds that the statute only applies to the predicate felony of arson, and cannot be applied to cross-burning. The court disagreed and affirmed the conviction.

*United States v. Brown*, 121 F.3d 700, 1997 WL 436741 (4th Cir. 1997) (unpublished)

The defendant pled guilty to violating 18 U.S.C. § 245(b)(2)(F) after he filled a two-liter soda bottle with gasoline and set it on fire in front of the Capital Lounge, a bar frequented by African Americans. The defendant's apparent motivation in setting the fire had been his belief that African Americans were "trying to take over." The court of appeals vacated his sentence and remanded for the district court to determine whether the defendant's acceptance of responsibility was exceptional enough to warrant a downward departure.

*United States v. Ramey*, 24 F.3d 602 (4th Cir. 1994)

The defendants were convicted of violating 18 U.S.C. § 241, 42 U.S.C. § 3631, and 18 U.S.C. § 844(h)(1) after they burned down the home of an interracial couple. The case contains a Commerce Clause analysis which is no longer good law. The defendants' convictions were vacated when the Supreme Court decided *Jones v. United States*, 519 U.S. 848 (2000), holding that § 844(i) does not reach an owner-occupied private residence. See *United States v. Ramey*, 217 F.3d 842 (4th Cir. 2000) (vacating § 844(i) conviction and remanding for resentencing).

*United States v. Piche*, 981 F.2d 706 (4th Cir. 1992)

The defendant was convicted on eight counts of violating 18 U.S.C. §§ 241 and 245(b)(2)(F) after he and his brother, who was convicted of a state murder charge, harassed and assaulted a group of Vietnamese men at a bar in Raleigh, killing one. The defendant appealed his conviction and the government appealed his sentence of 48 months' imprisonment. The court rejected defendant's challenge to the "death resulting" instruction and upheld the district court's instruction regarding whether the bar was a place of public accommodation. The court affirmed the conviction but vacated the sentence and remanded because the district court improperly departed from the guidelines.

*United States v. Roof*, 225 F. Supp. 3d 438 (D.S.C. 2016)

A district court in South Carolina upheld the constitutionality of 18 U.S.C. § 249(a)(1) in the case involving Dylann Roof's mass shooting at "Mother Emanuel" Episcopal Church. The district court held that § 249(a)(1) was a constitutional exercise of Congress's Thirteenth Amendment authority, holding that the provision "is an attempt to abolish what is rationally identified as a badge or incident of slavery."

*United States v. Hill*, 182 F. Supp. 3d 546 (E.D. Va. 2016)

The district court found that 18 U.S.C. § 249(a)(2) was unconstitutional as applied. The case involved an assault of a gay individual at an Amazon warehouse. The victim had been packaging boxes for shipping in interstate commerce when he was assaulted. The court recognized that § 249(a)(2) incorporated a jurisdictional element, and noted that the government had argued that the victim had been engaged in quintessentially economic activity when he was assaulted, which resulted in an estimated 1,710 packages not being delivered because of the assault. The court held, however, that if the court accepted this as a basis for jurisdiction, then the reach of [§ 249(a)(2)] would barely have an end, as the statute would cover any conduct that occurs at any commercial establishment." The court found that this would "effectively federalize commercial property and allow Congress to regulate conduct occurring on commercial premises, even when the conduct—here, violence based on discriminatory animus—has no connection to the commercial nature of the premises." The Court thus dismissed the indictment. As noted above, the Fourth Circuit reversed.

*United States v. Griffin*, 585 F. Supp. 1439 (M.D.N.C. 1984)

Defendants, who were allegedly members of the Ku Klux Klan and National Socialist Party of America who had conspired to heckle and disrupt an anti-Klan parade and cause bodily injury to the parade participants, were indicted on charges of conspiracy to violate 18 U.S.C. §§ 245(b)(2)(B) and (b)(4)(A). The defendants moved to dismiss the

indictment, arguing that the anti-Klan parade was neither an “activity” within the meaning of § 245(b)(2)(B), nor had it been “administered” by the city of Greensboro. The district court denied the motion, holding that the parade had been “administered” by the city of Greensboro because the city had taken an active role in controlling and managing the parade.

The court also held that the anti-Klan parade was an “activity” within the meaning of the statute, rejecting the defendants’ argument that § 245(b)(2)(B) was intended to reach only violent interference with tangible benefits and services of the city, such as fire and police protection and public housing. Looking to the plain language of the statute, the court found that the term “activity” was an inclusive term that expressed Congress’s intent to encompass state administered activities within the protection of the statute. The court determined that such activities encompassed events too transient in nature and too ephemeral to be designated services or programs, which quite reasonably included state-regulated parades. Additionally, the court found that the statute’s legislative history did not contradict the plain language of the statute. The statute’s history indicated that it had a broad remedial purpose and was intended to strengthen the government’s capability to meet the problem of civil rights violence. Accordingly, the court held that the attack on parade participants by the Ku Klux Klan epitomized the type of violence sought to be addressed by § 245.

### **Fifth Circuit**

*United States v. Cannon*, 750 F.3d 492 (5th Cir. 2014)

Defendants were convicted of violating 18 U.S.C. § 249(a)(1) after violently beating an African American man at a bus stop. On appeal, the court upheld the constitutionality of § 249(a)(1) as a valid exercise of Congress’s Thirteenth Amendment authority to identify and eradicate badges and incidents of slavery. A concurring opinion suggested that the Supreme Court should grant certiorari and consider its Thirteenth Amendment standard in light of the standards it had articulated for evaluating Fourteenth Amendment claims in *City of Boerne v. Flores*, 521 U.S. 507 (1997) and for evaluating Fifteenth Amendment claims in *Shelby Cty., Ala. v. Holder*, 133 S. Ct. 2612 (2013).

*United States v. Crimiell*, 547 Fed. App’x 633 (5th Cir. 2013) (unpublished)

The defendant pled guilty to violating 18 U.S.C. § 247 and making false statements after he damaged two Louisiana churches. The court of appeals affirmed his above-guidelines sentence, which included an upward variance, as reasonable.

*United States v. Mathis*, 476 Fed. App’x 22 (5th Cir. 2012) (unpublished)

The defendant pled guilty to violating 42 U.S.C. § 3631 and 18 U.S.C. § 924(c) after he fired into, and then set fire to, a home where three Hispanic men lived. The court of appeals upheld the defendant’s sentence after determining that the trial court did not commit procedural error.

*United States v. Scott*, 202 F.3d 265, 1999 WL 113195 (5th Cir. 1999) (unpublished)

The defendant pled guilty to violating 18 U.S.C. § 247(a)(1) but appealed her conviction, arguing that the statute violates the Establishment Clause. Citing the *Lemon*<sup>2</sup> test, the defendant alleged that § 247 does not have a secular legislative purpose, and has the primary effect of advancing or inhibiting religion. The court of appeals disagreed, holding as follows:

[§ 247] has a valid secular purpose, namely redressing the specific harms set out in the legislative history: the increasing violence and vandalism directed at houses of worship, the resulting interference with the free exercise of religion, and the absence of existing federal laws to prevent and address such violence and destruction . . . Furthermore, the protection afforded religious real property does not have the primary effect of advancing religion, as it constitutes neither an “endorsement” nor “promotion” of religion. The primary effect of § 247(a)(1) is on individuals who are prosecuted for engaging in criminal acts involving religion. Any benefit that inures to religious institutions as a result of § 247 is indirect and, therefore, does not endorse or promote religion.

*United States v. LeBaron*, 156 F.3d 621 (5th Cir. 1998)

The defendant was extradited from Mexico and convicted of violating 18 U.S.C. § 247(a)(2), among other charges, for his role in ordering the murders of individuals who had left his religious group. He appealed on several grounds, including the

---

<sup>2</sup> *Lemon v. Kurtzman*, 403 U.S. 602, 91 S. Ct. 2105 (1971).

admission at trial of his role in ordering another murder. The court affirmed his conviction.

*United States v. Sealed Appellant*, 123 F.3d 232 (5th Cir. 1997)

Two juveniles were convicted of violating 42 U.S.C. § 3631 after burning a cross near the home of an African American couple. The appeal raised issues unrelated to the scope or constitutionality of § 3631.

*United States v. Barlow*, 41 F.3d 935 (5th Cir. 1994)

Defendants were convicted under the original 1988 version of 18 U.S.C. § 247 for the murders of former cult members. On appeal, the defendants argued that § 247 did not apply because their “Church of the Lamb of God” was not a religion and that they did not “obstruct the victims’ free exercise of religion” as contemplated by the drafters of that statute.” The court first concluded that the defendants’ Church, a splinter Mormon sect, was a religion. “The mere fact that the beliefs of the Church may have derived from a perverse distortion of early Mormon beliefs or that it is a creed not practiced by multitudes does not prevent it from being classified as a ‘religion’ for the purpose of determining whether it is entitled to protection under the Free Exercise Clause.” As for the second claim, the jury was instructed that the “free exercise of religion” means “the victims’ voluntary choice to discontinue their membership in the Lamb of God.” The court found that the defendants “actions in assassinating their former co-religionists fall squarely within the ambit of § 247.”

*United States v. Pierce*, 5 F.3d 791 (5th Cir. 1993)

Defendant, a former Grand Dragon of the Ku Klux Klan, pled guilty to violating 18 U.S.C. § 241, 18 U.S.C. § 245(b)(2)(A), and 42 U.S.C. § 3631 after he planned with co-conspirators who then burned crosses at nine locations the day he began his sentence for a prior firearms conviction. The appeal raised issues unrelated to the scope or constitutionality of federal hate crimes.

*United States v. Greer*, 939 F.2d 1076 (5th Cir. 1991), reh’g en banc granted by 948 F.2d 934 and opinion reinstated in part on reh’g by 968 F.2d 433 (5th Cir. 1992)

Defendants, members of the Confederate Hammerskins, were convicted of violating 18 U.S.C. § 241 for conspiring to deprive black and Hispanic citizens of rights guaranteed by 42 U.S.C. § 2000a and conspiring to deprive Jewish citizens of rights guaranteed by 42 U.S.C. § 1982 after they conducted “park patrols” to clear a public park in Dallas of minorities. During the patrols, they “chased, beat, and assaulted any nonwhites they found.” The evidence also showed that they vandalized Temple Shalom in Dallas and the Jewish Community Center by spray-painting the walls with anti-Semitic graffiti, shooting out the glass on the windows and doors of the temple and breaking windows and doors with baseball bats. The court of appeals held that the evidence properly established that the defendants engaged in two separate conspiracies. In addition, the court, reasoning that “to hold” property can also mean “to use” property, rejected defendants’ argument that the temple and community center were not “citizens” within the meaning of the Constitution and thus not covered by § 241.

*United States v. Johns*, 615 F.2d 672 (5th Cir. 1980)

Defendants, all Klan members, were convicted of violating 18 U.S.C. § 245(b)(5), 18 U.S.C. § 371 (general conspiracy), and 42 U.S.C. § 3631 after shooting into the homes of African American families during a campaign to discourage interracial dating and to disrupt NAACP activities promoting affirmative action. The court of appeals upheld their convictions, noting that the “evidence adduced at trial demonstrates that in attacking the NAACP leaders the defendants intended forcibly to discourage the NAACP’s efforts to secure better employment and housing opportunities for blacks.” The statute “clearly warrants prosecuting individuals who attempt to interfere with such efforts.” The court also concluded that the “presence of other motives, given the existence of the defendants’ motive to end interracial cohabitation, does not make [the defendants’] conduct any less a violation of 42 U.S.C. § 3631.”

*Hayes v. United States*, 464 F.2d 1252 (5th Cir. 1972)

Defendants were convicted of violating 18 U.S.C. §§ 241 and 1509 (obstruction of court order) for their role in setting off explosive charges in the parking lot of a school to prevent desegregation. The court of appeals ruled that the right of black students to attend school without regard to race or color is secured by Title IV of the Civil Rights Act of 1964, 42 U.S.C. § 2000c(b), and thus the conspiracy count stated an offense, even though it did not include an allegation of state action. “Because the right of black students to attend public schools without regard to race or color is secured by a federal statute, Count 1 of the indictment stated an offense against the United States.” The court did not reach the United States claim that the right to attend school was also protected by the Thirteenth Amendment.

*Wilkins v. United States*, 376 F.2d 552 (5th Cir. 1967)

The court of appeals recognized a conspiracy among purely private individuals who assaulted those marching for voting rights between Selma and Montgomery, Alabama. Although the acts of the defendants did not implicate a pending federal election, the court held that “any citizen of the United States participating in the march was exercising an attribute of national citizenship, guaranteed by the United States.” For this reason, the court explained, “a conspiracy against those participating [in the march] would be a violation of 18 U.S.C. § 241.”

*United States v. Harris*, 128 F. Supp. 3d 957 (N.D. Miss. 2015)

The defendant pled guilty to violating 18 U.S.C. §§ 245(b)(2)(A) and (C) after he and two other men, all members of a fraternity at the University of Mississippi, drank late into the evening and then, desiring to “create a sensation on campus using a Confederate flag,” draped an old Georgia state flag (which contained a Confederate battle flag) over and hung a rope around the neck of the statue of James Meredith, the first African-American student to be admitted to the then-segregated university. The court of appeals remanded the case for re-sentencing after determining that the hate crime motivation adjustment constituted “double counting” when applied to the hate crime offense set forth at § 245(b)(2).

### **Sixth Circuit**

*United States v. Miller*, 767 F.3d 585 (6th Cir. 2014)

The court of appeals reversed conviction in the *Mullet* case, described below, finding that the district court did not apply the intervening Supreme Court case, *Burrage v. United States*, 134 S. Ct. 881 (2014), which required that the jury be instructed that it must find “but for” causation, and that, to find a defendant guilty of violating 18 U.S.C. § 249, the jury must find that without religious motivation the defendant would not have acted.

*Glenn v. Holder*, 690 F.3d 417 (6th Cir. 2012)

Ministers and pastors brought a civil action seeking to enjoin enforcement of 18 U.S.C. § 249(a)(2). The ministers and pastors claimed that the law would have a chilling effect on their ability to preach against homosexuality. The court of appeals held that they did not have standing to challenge the law because they stated that they did not intend to engage in violent acts or encourage others to do so.

*United States v. Mardis*, 600 F.3d 693 (6th Cir. 2010)

The defendant was indicted for violating 18 U.S.C. § 245 for murdering an African American on account of the victim’s race and color as well as the victim’s employment by a governmental entity. The appeal raised issues unrelated to the scope or constitutionality of federal hate crimes.

*United States v. Vartanian*, 245 F.3d 609 (6th Cir. 2001)

Three real estate agents had finalized the sale of a home to an African American family when the defendant, a white neighbor, approached and threatened to kill the realtors. He was convicted of violating 42 U.S.C. §§ 3631(a) and (b)(2). The defendant argued on appeal that he was improperly convicted because he did not directly threaten the African American family. The court held that § 3631 also reaches threats to real estate agents. “The fact that a threat or act of intimidation was not addressed directly to the protected individual does not mean that those words or conduct cannot or will not have the effect desired by the defendant . . . In this case, where the obvious intent of the defendant was also to protest the action of the individual buyers, not just of the agents themselves, we conclude that a rational trier of fact would be justified in inferring that the import of the threat would be transmitted to the buyers.” The court rejected the defendant’s argument that his two convictions on two grounds for one act were multiplicitous. The court held that § 3631(a) and § 3631(b)(1) require proof of distinct elements.

*United States v. McGee*, 173 F.3d 952 (6th Cir. 1999)

The defendant was convicted of violating 18 U.S.C. § 245(b)(4)(A) after assaulting a black man who was trying to enter a bar. The defendant raised several sufficiency-of-the-evidence issues on appeal, including that because the victim was drunk, there was a legitimate reason to deny him entrance. In upholding his conviction, the court reasoned that the defendant “appears to believe that so long as there was a legitimate reason to exclude [the victim], [the defendant’s] true motivations in excluding [the victim] were not relevant. This is not an accurate statement of the law. Instead, the law provides that so long as racial animus is a substantial reason for a defendant’s conduct, other motivations are not factors to be considered.”

*United States v. Mahan*, 190 F.3d 416 (6th Cir. 1999)

The defendant was convicted of violating 42 U.S.C. § 3631 after he littered the yard of an African American family with about 100 copies of a hate flyer that threatened physical violence. The appeal raised issues unrelated to the scope or constitutionality of § 3631.

*United States v. Sauer*, 198 F.3d 248, 1999 WL 1021582 (6th Cir. 1999) (unpublished)

The defendant, a priest, pled guilty to violating 18 U.S.C. § 247 after he set fire to the curtains behind his church's altar. The court of appeals affirmed the defendant's sentence because the district court recognized its opportunity to depart downward from the sentencing guidelines, but chose not to do so under the circumstances of the case.

*United States v. Johnson*, 152 F.3d 553 (6th Cir. 1998)

The defendant, who is black, pled guilty to one count of damaging religious property in violation of 18 U.S.C. § 247(c), after he drove a stolen automobile up to a church which had a predominantly white congregation and set the vehicle on fire; the fire spread to the church. In his confession, the defendant stated that, "he was doing the will of Satan by burning the church which would cause racial tension between blacks and whites." The court of appeals remanded the case for resentencing after concluding that an upward departure was inappropriate.

*United States v. Bakenhus*, 116 F.3d 1481, 1997 WL 345957 (6th Cir. 1997) (unpublished)

The defendant pled guilty to violating 18 U.S.C. §§ 241, 924(c), 844(i), and 42 U.S.C. § 3631(a) after he and others threw explosives at and fired into the home of an African American family; broke into, damaged, and set fire to the home of another African American family; and, set fire to a building housing an historic African American fraternal organization. He appealed his sentence, arguing in part that the race of his victims was an element of the underlying charge and thus using race to characterize the victims as vulnerable amounted to double-counting. Citing *United States v. Salyer*, 893 F.3d 113 (6th Cir. 1989) (§ 241 case), the court held that "the minority status of the victims in Clarksville, a predominantly white community, and [the defendant's] purposeful attack against them because of their minority status, justifies the district court's determination that these victims were uncommonly vulnerable to the defendant's acts."

*United States v. Brown*, 49 F.3d 1162 (6th Cir. 1995)

The defendant was convicted of violating 18 U.S.C. § 241 for his role in the drive-by shooting of a synagogue. On appeal, he argued that because the synagogue was owned by a corporation and not by citizens, there could be no violation of 42 U.S.C. § 1982. The court held that the United States "need not prove that the defendant actually knew it was a constitutional right being conspired against or violated." Following *Greer*, the court concluded that to "hold" property includes the right to "use" property. "[N]on-owners of property who nevertheless have an interest in using or holding that property have a viable property interest protected under Section 1982."

*United States v. Wiegand*, 45 F.3d 431, 1994 WL 714347 (6th Cir. 1994) (unpublished)

The defendant appealed his 42 U.S.C. § 3631 conviction and sentence for setting fire to a house and causing injury to a firefighter. An issue on appeal was whether the penalty provision of § 3631 was limited to a particular group of individuals—i.e., those who are exercising housing rights. The court, citing *United States v. Hayes*, 589 F.2d 811, 821 (5th Cir. 1979) (§ 242 case), held that "injury to a firefighter is a foreseeable result of arson, which is the criminal conduct at issue here." Nor did it matter that § 844(i) already provided identical protection for firefighters because, the court reasoned, "it is well within Congress's discretion to afford persons the same protection in more than one statutory provision."

*United States v. Gresser*, 935 F.2d 96 (6th Cir. 1991)

The defendants were convicted of violating 18 U.S.C. § 241, 42 U.S.C. § 3631, and 18 U.S.C. § 844(h)(1) after they and their accomplices burned a cross following an altercation with African American youths. One defendant argued on appeal that the evidence was insufficient to support his conviction because his "rage was directed at his attackers and not blacks in general." The court held the evidence was sufficient, stressing that the defendants expressed their rage in entirely racial terms. The court also rejected the argument that § 844(h) applied only to arson and not to other uses of fire.

*United States v. Salyer*, 893 F.2d 113 (6th Cir. 1989)

The defendant pled guilty to violating 18 U.S.C. § 241 after burning a cross in the yard of an African American family's home. He appealed the district court's decision to increase his sentence by two points for victim vulnerability. The court

held that because the victims were particularly susceptible to the crime, and because race is not incorporated into the definition of the civil rights conspiracy statute, they could be considered vulnerable victims for the purposes of sentencing the defendant.

*United States v. White*, 788 F.2d 390 (6th Cir. 1986)

The defendant was convicted of violating 18 U.S.C. § 241 and 42 U.S.C. § 3631 after conspiring with others to burn down the home of an African-American family, which was under construction across the street from the defendant's home. The court of appeals upheld the conviction against a challenge to the sufficiency of the evidence.

*United States v. Ebens*, 800 F.2d 1422 (6th Cir. 1986), abrogated on other grounds by *Huddleston v. United States*, 485 U.S. 681 (1988)

The defendant was convicted of violating 18 U.S.C. § 245(b)(2)(F) after violently killing a Chinese man following an altercation that began at a topless bar and continued outside after they were ejected from the club. The court of appeals rejected the defendant's claims that there was insufficient evidence to establish that he was motivated because of the race, color, and national origin of the victim, or that his purpose was to injure, intimidate, and interfere with the victim's right to enjoy a place of public accommodation. The court, however, reversed the defendant's conviction and remanded for a new trial because of evidentiary errors.

*United States v. Fruit*, 507 F.2d 194 (6th Cir. 1974)

Defendants, who planned to dynamite school busses and to fire at the buses with a weapon, were convicted of violating 18 U.S.C. § 241 for conspiring to injure, oppress, threaten, and intimidate black students in Michigan in their right to attend school without regard to race. Defendants argued on appeal that there was no state involvement, which is required for a Fourteenth Amendment violation. Relying on the Fifth Circuit's decision in *Hayes*, the court of appeals held that the acts of the defendants violated Title IV of the Civil Rights Act of 1964.

*United States v. Doggart*, 2017 WL 2416920 (E.D. Tenn. 2017)

The defendant was convicted by a jury of violating 18 U.S.C. § 247(a)(1), solicitation to commit arson, and making threats in interstate commerce after he solicited and discussed with others plans to damage and destroy a mosque, school, and other facility in an Islamic community in New York. The district court granted defendant's motion for acquittal with respect to the threat charges, but held that sufficient evidence supported his § 247 and solicitation to commit arson convictions.

*United States v. Jenkins*, 2012 WL 4887389 (E.D. Ky. 2012)

The defendants were indicted for violating 18 U.S.C. § 249(a)(2) after they lured their victim into a vehicle and drove him to a deserted location in order to assault him based upon his sexual orientation. The district court, while critical of § 249(a)(2), held that the indictment was constitutional on its face because Congress validly passed it pursuant to its Commerce Clause authority. It also found that the statute was constitutional "as applied" to the allegations in the indictment, which alleged that the crime was committed through the use of a motor vehicle and interstate highways. These allegations, the court held, were sufficient to bring the defendants' conduct within the scope of the Commerce Clause.

*United States v. Mullet*, 868 F.Supp.2d 618 (N.D. Ohio 2012)

Defendants, members of an Amish sect, were charged with violating 18 U.S.C. § 249(a)(2) after they violently broke into the homes of other members of the Amish community whom they deemed were not faithfully following the religion, and forcefully sheared the hair of their victims, causing bodily injury. In response to the defendants' constitutional challenge to the indictment, the district court held that § 249(a)(2) was constitutional *on its face* because Congress passed the statute pursuant to a valid exercise of its Commerce Clause authority. It also found the statute was constitutional *as applied* to the allegations in the indictment. It held that the fact that the crime was alleged to have been committed with weapons that had traveled in commerce, with hired vehicles, and by luring victims through the mail was sufficient to bring the defendants' conduct within the scope of the Commerce Clause. The court also held that § 249 applied to acts of intra-religious violence, and that it did not infringe on the defendants' First Amendment rights.

*United States v. Fredericy*, No. 1:06-00035 (Plea Agreement) (N.D. Ohio filed Oct. 5, 2006)

Defendants pled guilty to violating 18 U.S.C. § 241, 42 U.S.C. § 3631, and to making false statements after they conspired to injure and intimidate African American residents into leaving their neighborhood in Cleveland, Ohio. Specifically, one of the defendants, with the other's encouragement, released mercury onto the front porch of the home of

an interracial couple and their four children.

### **Seventh Circuit**

*United States v. Milbourn*, 600 F.3d 808 (7th Cir. 2010)

The defendant was convicted of conspiring to deprive a family of their right to occupy a dwelling free from intimidation based on race, in violation of 18 U.S.C. § 241, 42 U.S.C. § 3631, and other statutes, after he and another man built a cross, transported it to the home of a couple with three bi-racial children living in a predominantly white neighborhood, dug a hole in the front yard, planted the cross, doused it with gasoline, set it on fire, and then laughed while they watched it burn. The family, terrified and concerned for the children's safety, eventually moved from the neighborhood. The court of appeals held that the evidence was sufficient to prove that the defendant's actions were motivated by the race of the victims and was intended to intimidate and interfere with their housing rights. "Of all the things to burn in someone's yard, [defendants] chose a cross. Of all the places to burn that cross, they chose the front yard of a rented house that served as the home for three biracial children." After reciting the history and meaning of cross-burning, the court concluded that the evidence was sufficient to establish all elements of the crime.

*United States v. Dropik*, 476 F.3d 471 (7th Cir. 2007)

The defendant pled guilty to two counts of violating 18 U.S.C. §§ 247(c) and 247(d)(3) for racially-motivated arson which damaged religious property. The appeal raised issues unrelated to the scope or constitutionality of § 247.

*United States v. Craft*, 484 F.3d 922 (7th Cir. 2007)

The defendant was convicted of violating 18 U.S.C. § 844(h) (use of fire to commit a felony) where the underlying felony was 42 U.S.C. § 3631, after burning several buildings and homes in Indiana. On appeal, the defendant argued that there was insufficient evidence to support finding that the fires were motivated by racial animus. He contended that he set fire to one of the homes because the owner owed him money. The court ruled that "[t]he government was not required to prove, however, that racial animus was [the defendant's] sole motivation in setting the fire. Rather, it was only required to prove that the victims' race or ethnicity partially motivated [the defendant's] crimes." The defendant also argued that he did not interfere with the victims' housing rights because one family was not living at the residence at the time of the arson and the other family had moved out before the actual arson. The court disagreed, noting that § 3631 could be violated before owners physically reside in a property and that, by its terms, it prohibits interfering with a person who "is or has been" renting a dwelling. Some of the decision's rationale has been vitiated by *Burrage v. United States*, 134 S. Ct. 881 (2014).

*United States v. Flowers*, 389 F.3d 737 (7th Cir. 2004)

The defendant, who had participated in a cross-burning, pleaded guilty to violating 42 U.S.C. § 3631. The appeal raised issues unrelated to the scope or constitutionality of § 3631.

*United States v. Colvin*, 353 F.3d 569 (7th Cir. 2003) (en banc)

The defendant was convicted of violating 18 U.S.C. § 241, 18 U.S.C. § 844(h)(1), and 42 U.S.C. § 3631 after burning a cross in front of the home of a Puerto Rican man and carrying a firearm during the incident. The defendant asserted on appeal that his conviction under § 844(h)(1) (using of fire to commit a felony) violated the Double Jeopardy Clause to the extent that it was based on his conviction under § 3631 (which itself prescribes a greater punishment when fire is used). The court concluded that Congress intended such cumulative punishment in a 1988 amendment to § 844(h)(1). However, the court ruled that a conspiracy conviction under § 241 could not be used as a predicate felony to support a conviction for committing a felony by using fire. This portion of the court's decision overruled *United States v. Hartbarger*, 148 F.3d 777 (7th Cir. 1998) (see below) and *United States v. Hayward*, 6 F.3d 1241 (7th Cir. 1993) (see below).

*United States v. Hartbarger*, 148 F.3d 777 (7th Cir. 1998), overruled in part by *United States v. Colvin*, 353 F.3d 569 (7th Cir. 2003)

The defendants were convicted of violating 18 U.S.C. § 241, 42 U.S.C. § 3631, and 18 U.S.C. § 844(h)(1) for burning a cross on the property of an interracial couple and their children. The court of appeals ruled that the district court did not abuse its discretion when it limited testimony that the defendants did not understand the historical significance of cross-burning because, as children, they lived in isolation from people and the media. The court also held that evidence of the victims' reaction to the cross-burning could be introduced as evidence of the defendants' intent so long as the jury is

instructed that it is not conclusive evidence.

*United States v. Rogers*, 45 F.3d 1141 (7th Cir. 1995)

The defendant was convicted of violating 18 U.S.C. § 241, 42 U.S.C. § 3631, and other statutes after terrorizing an African American family by shooting at them, ripping out their telephone line, yelling racial epithets, breaking an awning post to their home, and brandishing brass knuckles and a knife. The appeal raised issues unrelated to the scope or constitutionality of federal hate crimes.

*United States v. Montgomery*, 23 F.3d 1130 (7th Cir. 1994)

The defendant was convicted of violating 18 U.S.C. § 241 and 42 U.S.C. § 3631 after burning a cross in front of a shelter for homeless veterans, of whom 60% were African American. The court of appeals summarily rejected arguments that there was insufficient evidence to support a conviction and that the defendant received ineffective assistance of counsel.

*United States v. Sowa*, 34 F.3d 447 (7th Cir. 1994)

The defendant was convicted of violating 18 U.S.C. § 371 (general conspiracy) and 18 U.S.C. § 245(b)(2)(B) after he conspired to interfere with the rights of two African American men to use the streets and sidewalks of the city because of their race, and then used a baseball bat to brutally bludgeon them. The appeal raised issues unrelated to the scope or constitutionality of § 245(b)(2)(B).

*United States v. Hayward*, 6 F.3d 1241 (7th Cir. 1993), overruled in part by *United States v. Colvin*, 353 F.3d 569 (7th Cir. 2003)

The defendants were convicted of violating 18 U.S.C. § 241, 42 U.S.C. § 3631, 18 U.S.C. § 844(h)(1), and other statutes after burning a cross in front of the home of a white couple who entertained African American visitors. The court of appeals rejected the defendants' argument that cross-burning was protected speech.

*United States v. Myers*, 892 F.2d 642 (7th Cir. 1990)

Defendants were convicted of violating 18 U.S.C. § 241 and 42 U.S.C. § 3631 after firebombing an African American family's car in a successful attempt to force them to move from the area. The conviction was vacated and remanded for a hearing by the district court on the question of whether a defendant's counsel was ineffective at trial. On remand, the district court rejected the defendant's claim of ineffective counsel, and the court of appeals affirmed his conviction in *United States v. Myers*, 917 F.2d 1008 (7th Cir. 1990).

*United States v. Redwine*, 715 F.2d 315 (7th Cir. 1983)

The defendants were convicted of violating 18 U.S.C. § 241, 42 U.S.C. § 3631, and other statutes after firebombing the house of an African American family a month after they moved into the neighborhood. The court of appeals rejected defendants' contention that they were convicted on insufficient, circumstantial evidence. The court also held that the defendants' acts of throwing rocks through the victims' windows and pronouncing that the family should be "burned out" were sufficient to sustain their convictions for willfully intimidating and interfering with the family because of their race and occupation of the home. Finally, the court held that a proven conspirator is responsible for the substantive offenses based on the overt acts of fellow conspirators, thus upholding the conviction of one defendant for aiding and abetting the firebombing.

*United States v. Nix*, 417 F. Supp. 2d 1009 (N.D. Ill. 2006)

The defendant was charged with violating 42 U.S.C. § 3631 after detonating an explosive device inside a vehicle parked in front of the home of a family of Arab descent. The parties submitted conflicting jury instructions on the issue of the amount of racial motivation required for a § 3631 conviction. The court rejected the idea that only incidental racial motivation was required. The court proposed to define the "because of" element as follows: "The government must prove that the defendant acted 'because of' the race or national origin of [the victim] and 'because' [the victim] was occupying a dwelling. This means that the government must prove that both [the victim's] race or national origin and her occupancy of a dwelling, were substantial motivating factors in the defendant's actions. The government is not required to prove that these were the defendant's sole motivations."

*United States v. Nicholson*, 185 F. Supp. 2d 982 (E.D. Wis. 2002)

The defendant, charged with violating 18 U.S.C. § 241, 42 U.S.C. § 3631, and 18 U.S.C. § 844(h)(1) for his role in the firebombing of a house occupied by a Hmong family, filed a motion to dismiss arguing that both § 241 and § 3631

exceeded the scope of Congress' power under the Commerce Clause and the Thirteenth Amendment. The defendant argued that Congress is without authority to criminalize activity where the only link to interstate commerce is "occupation" of a dwelling. The court rejected the defendant's argument, relying on the aggregate effects on a national housing market. The court also found that the Fair Housing Act was an "exercise of congressional power under the thirteenth amendment to eliminate the badges and incidents of slavery."

*United States v. Bronk*, 604 F. Supp. 743 (W.D. Wis. 1985)

The defendants were charged with violating 18 U.S.C. § 245(b)(2)(F) and 18 U.S.C. § 371 (general conspiracy) and moved to dismiss their indictment on the ground that the tavern in which the acts alleged in the indictment were said to have occurred was not a facility which serves the public within the meaning of that term in § 245(b)(2)(F) because the tavern was not open to people younger than the state drinking age pursuant to Wisconsin law. With no discussion, the court agreed with the magistrate's common sense construction of the word "public" to include all persons of the community not otherwise precluded by law from entering the premises. However, the court dismissed the indictment without prejudice for failure to comply with the certification requirement.

### **Eighth Circuit**

*United States v. Maybee*, 687 F.3d 1026 (8th Cir. 2012)

The defendant was convicted of violating 18 U.S.C. § 249(a)(1) after he and his companions confronted a group of Mexican Americans at a convenience store, calling them racial slurs. Upon seeing the victims drive away in a sedan, the defendant and his companions pursued them in the defendant's pickup truck. Ultimately, the defendant rammed the victim's sedan with his pickup truck and then executed a "pit maneuver" designed to cause the driver of the sedan to lose control. The sedan crashed through a fence and burst into flames, seriously injuring all five victims. The court of appeals upheld the constitutionality of 18 U.S.C. § 249(a)(1), finding that Congress had Thirteenth Amendment authority to enact it. The court rejected the defendant's argument that Congress could not pass legislation under the Thirteenth Amendment except to enforce some other federally-protected right (e.g., the right to vote; the right to fair housing).

*United States v. Sandstrom*, 594 F.3d 634 (8th Cir. 2010)

The defendants were convicted of violating 18 U.S.C. § 245(b)(2)(B) and other offenses for shooting on two separate occasions, and eventually killing, an African American man who was walking down a public street. The court of appeals rejected defendants' constitutional challenge to § 245, holding that in enacting the statute, Congress acted well within its authority under both section 2 of the Thirteenth Amendment and the Commerce Clause. The court also rejected several arguments raised by defendants that were unrelated to civil rights issues.

*United States v. Weems*, 517 F.3d 1027 (8th Cir. 2008)

Defendants were convicted of violating 18 U.S.C. § 241 for their involvement in burning a cross outside the home of one of the defendant's African-American neighbor. On appeal, the court ruled that "because the jury found beyond a reasonable doubt that [the defendants] selected the victim because of his race, the district court should have applied the three-level hate crime enhancement when calculating the correct guidelines range," and that applying a hate crime sentencing enhancement for the violation of a hate crime statute "is not duplicative because the race of the victim is not an element of § 241, and it is not incorporated in the applicable base offense level."

*United States v. Corum*, 362 F.3d 489 (8th Cir. 2004)

The defendant was convicted of violating 18 U.S.C. § 247(a)(2) and other offenses after leaving threatening voice mail messages at three synagogues. The court of appeals held that the Church Arson Prevention Act was constitutional under the three-part Establishment Clause test in *Lemon*, and further held that the statute was enacted pursuant to a valid exercise of Congress's Commerce Clause authority. The court also held, without analysis, that the record "reveals that the government presented sufficient evidence for the jury to have determined the offense (threatening phone calls) affected interstate commerce."

*United States v. Pospisil*, 186 F.3d 1023 (8th Cir. 1999)

Defendants were convicted of violating 18 U.S.C. § 241, 42 U.S.C. § 3631, and other statutes after they burned a cross in the front yard of a Cape Verdean family—whom the defendants thought were African American—and also fired shots into the air and shouted racial epithets. Their convictions were affirmed, and the court of appeals rejected an argument that

the district court impermissibly refused to allow the defense to peremptorily strike African American citizens from the jury. The court held that there is no exception to *Batson v. Kentucky*, 476 U.S. 79 (1986), in racial hatred cases. (*Batson* forbid the discriminatory use of peremptory strikes in jury selection.) One defendant's sentencing enhancement for "vulnerable victim" was upheld because he was aware that children lived in the house and that the family was new to town. The enhancement was stricken for the other defendant, however, because the government had not established that he was aware of these facts.

*United States v. Dunnaway*, 88 F.3d 617 (8th Cir. 1996)

The defendants were convicted of violating 18 U.S.C. § 245(b)(2)(B) after they left a party to assault any black man they could find. They found the victim in a public park talking with his wife, who was white. The defendants attacked the victim, kicking him repeatedly in the head and body. During the attack, the defendants used racial slurs, and one of the defendants identified himself as a skinhead. After returning to the party, the defendants boasted that they had beaten a black man because he had been sitting in a park with a white woman. The court of appeals held that it was proper for the court to admit testimony that one of the defendants identified himself as a skinhead because the crime involved elements of racial hatred. The court also held that evidence of a defendant's racist views, behavior, and speech were relevant and admissible to show discriminatory purpose and intent. The court disagreed with defendants' argument that the aggravated assault guideline used at sentencing was inapplicable and that the bottle and boots used in the assault were not dangerous weapons.

*United States v. J.H.H.*, 22 F.3d 821 (8th Cir. 1994)

The court of appeals affirmed the convictions, based on violations of 18 U.S.C. § 241 and 42 U.S.C. § 3631, of three juvenile men who burned crosses near an African American family's home four months after they moved in. The court rejected the contention that § 3631 violated the First Amendment and held that there was sufficient evidence to find that cross-burnings were meant to be threatening and cause fear of the imminent use of force. The court also held that admitting expert testimony about skinhead organizations was harmless because there was other ample evidence to support conviction.

*United States v. McDermott*, 29 F.3d 404 (8th Cir. 1994)

The defendant was convicted of violating 18 U.S.C. § 245(b)(2)(B) after he and a group of teenagers had attempted, for approximately a year, to keep black individuals out of a public park by brandishing weapons, veering cars towards individuals, chasing individuals, spitting on children, and ultimately burning a fifteen-foot cross in the park. The indictment charging the defendant with § 245(b)(2)(B) specified only the cross-burning. On appeal, the court recognized that burning a cross may be protected expression under the First Amendment; however, the court explained that the defendant could be convicted for the protected activity of burning a cross if it was done either to incite unlawful violence or to threaten. The court held that the challenged jury instruction failed to explain the difference between protected expressive activity and unprotected threats or incitement to imminent lawless action. Moreover, the instruction failed to mention that the defendant must have acted with specific intent to threaten the use of force. The court explained that the trial judge permitted the jury to conclude that a threat of force was used if it found that the defendant "burned a cross in order to threaten." The court reasoned that, by wording the instruction in permissive terms, the trial judge allowed the jury to convict without finding that the defendant burned the cross with the intent to threaten *the use of force* or at least cause blacks to reasonably fear the imminent use of force or violence. Accordingly, the court reversed and remanded.

*United States v. Lee*, 935 F.2d 952 (8th Cir. 1991) and 6 F.3d 1297 (8th Cir. 1993) (en banc)

The defendant was charged with violating 18 U.S.C. § 241, 42 U.S.C. § 3631, and 18 U.S.C. § 844(h)(1) for constructing and burning a cross on a hill near an apartment complex occupied by numerous African Americans. The defendant was convicted of violating §§ 241 and 844(h)(1) but acquitted of the § 3631 charge. On appeal, the defendant argued that § 844(h)(1) was not intended to apply to the conduct at issue, and a panel of the court of appeals reversed his conviction on this count. Specifically, the panel held that § 844(h) only applied to the underlying crime of arson and not to a cross-burning.

*United States v. Bledsoe*, 728 F.2d 1094 (8th Cir. 1984)

The defendant, who regularly went to a public park with his companions to harass homosexuals, was convicted of violating 18 U.S.C. § 245(b)(2)(B) after he struck a white man, who eventually ran away, and then struck a black man with a baseball bat. That black man also ran away, but the defendant gave chase, caught up to him, and repeatedly struck the man on the top of his head, crushing his skull and killing him. On appeal, the court rejected the defendant's argument

that the jury instructions suggested that a violation of § 245 could be based on actions that were motivated only incidentally by race. The court also rejected the defendant's claim that the evidence supported a finding that he attacked the victim because of his sexual orientation rather than race. The court held that the evidence sufficiently established that the defendant had a history of violently attacking blacks, and further, that this attack in particular was motivated by racial hatred. Importantly, the record contained admissions by the defendant boasting about the murder in racially derogatory terms, and the government introduced circumstantial evidence that the white man, whom the defendant believed to be a homosexual, was allowed to escape after a single strike, but the black victim was beaten, pursued, caught, and killed.

*United States v. Metcalf*, No. 15-CR-1032-LRR, 2016 WL 827763 (N.D. Iowa Mar. 2, 2016)

The defendant was charged with violating 18 U.S.C. § 249 for assaulting an African American man in a bar. After getting into an argument with the victim's female friends, the defendant directed racial slurs at the victim and his friends, told other patrons that he hated black people, bragged to the bar's owner about being involved in cross-burnings, and flashed his swastika tattoo. Later that night, after hours of taunting, the defendant attacked the victim's female friend. When the victim intervened to protect her, the defendant's friends knocked him out. As the victim lay barely conscious on the floor of the bar, the defendant walked over to him and repeatedly kicked and stomped on his head. The district court upheld § 249(a)(1) as a valid exercise of Congress's Thirteenth Amendment authority, after canvassing all other cases previously issued.

### **Ninth Circuit**

*United States v. Cazares*, 788 F.3d 956 (9th Cir. 2015)

Between 1995 and 2001, several members of the Avenues 43, a Latino street gang operating in the Highland Park neighborhood of Los Angeles, directed racial slurs, threats, assaults, and general harassment toward African American residents of the neighborhood; ultimately, they murdered an African American resident—all with the intent to drive African American residents from their homes. Four defendants were charged, tried, and convicted of conspiring to intimidate African American citizens in the Highland Park neighborhood and to deprive them of their right to occupy a dwelling free from intimidation based on race, a right protected by 42 U.S.C. § 3631, in violation of 18 U.S.C. § 241; three of the four defendants were also convicted of violating 18 U.S.C. § 245(b)(2)(B) and weapons charges. The appeal raised issues unrelated to federal hate crimes.

*United States v. Silva*, 428 Fed. App'x 737 (9th Cir. 2011) (unpublished)

The defendants, a married couple, were convicted of violating 18 U.S.C. § 245(b)(2)(B) after they verbally harassed and physically assaulted beach-goers of Indian descent. The appeal raised issues unrelated to the scope or constitutionality of § 245.

*United States v. Smith*, 2010 WL 510634 (9th Cir. 2010) (unpublished)

The defendant was convicted of violating 42 U.S.C. § 3631 after he made repeated threats, over a CB radio, to go to the home of an African American victim, burn a cross, hang the victim in a tree, and rape the victim's wife. At some point, the victim told the defendant to "come on over," and the defendant did so; he arrived with several other men and began verbally harassing the victim. The victim called the police, who broke up the incident before any violence actually occurred. The conviction was upheld on appeal. The appellate court opinion dealt with criminal procedure and sentencing issues. Significantly, the court held that, to obtain a sentencing enhancement for racial motivation, the government need not prove that race was a primary motivating factor, but that, instead, it was sufficient to show the same level of motive required for conviction in the first instance (the jury had been instructed that to convict, it must determine that race was a substantial—not a primary—motivating factor). The court's decision is likely vitiated by *Burrage v. United States*, 134 S. Ct. 881 (2014).

*United States v. Armstrong*, 620 F.3d 1172 (9th Cir. 2010)

The defendant was convicted of violating 18 U.S.C. § 245(b)(2)(F) after he and others brutally assaulted an African American man outside of a shopping center. The court of appeals upheld an upward adjustment to the defendant's sentence calculation, pursuant to U.S.S.G. § 3A1.1(a), because the victim was selected based on race.

*United States v. Allen*, 341 F.3d 870 (9th Cir. 2003)

The defendants, white supremacists, were convicted of violating 18 U.S.C. § 245(b)(2)(B) and 18 U.S.C. § 241 after

engaging in a “park patrol” intended to drive minorities out of a local park. The court of appeals rejected defendants’ arguments that the park did not satisfy elements of § 245 because it was closed at the time of the attack, and that it was not a public accommodation because it did not provide sources of entertainment. The court disagreed, finding that there was ample evidence that the park was a place for performances, exhibitions, and other sources of entertainment. The court also upheld the admission at trial of skinhead and white supremacist evidence, including color photographs of their tattoos, Nazi-related literature, group photographs, and skinhead paraphernalia, holding that, although the evidence was prejudicial, it was not unfairly so and it properly had been admitted in order to prove racial animus.

*United States v. Machado*, 195 F.3d 454 (9th Cir. 1999)

The defendant was convicted of violating 18 U.S.C. § 245(b)(2)(A) after twice sending a racist, profane email message from the computer lab at a university to approximately sixty Asian American students. The appeal raised issues unrelated to the scope or constitutionality of § 245.

*United States v. Baird*, 189 F.3d 475 (9th Cir. 1999) (mem.) (unpublished)

The defendant, a white supremacist, was convicted of violating 18 U.S.C. § 241 and 18 U.S.C. § 245(b)(2)(F) after he and several friends beat two men, one black and one Hispanic, in the parking lot of a 7-11 store. On appeal, the court held that there was sufficient evidence to establish that the defendant specifically intended to prevent the victims from using the services and facilities of the 7-11 because of the victims’ race, and that the store and its facilities constituted a public accommodation within the meaning of the statute.

*United States v. Makowski*, 120 F.3d 1078 (9th Cir. 1997)

The defendant was convicted of violating 18 U.S.C. § 245(b)(2)(B) after he physically assaulted and injured a Hispanic man at a public park while the victim watched his daughter play on a playground. Before, during, and after the assault, the defendant used racial epithets. In holding that § 245(b)(2)(B) was not void for vagueness, the court of appeals stated that the statute requires proof of the specific intent to interfere with a federally-protected activity on the basis of race.

According to the court, racial animus must be a motivating factor in the use or threat of force. Because the statute requires that an individual act willfully, the statute clearly excludes situations involving the incidental use of racial epithets during an altercation.

*United States v. Sanders*, 41 F.3d 480 (9th Cir. 1994)

The defendant was convicted of violating 42 U.S.C. § 3631 and of sending threatening communications after mailing letters replete with racial epithets to a local chapter of the NAACP, which also housed the chapter president’s home. The court of appeals held that it was not error for the district court to hold the defendant ineligible for a reduction of sentence because his activities were but a “single instance” of conduct “evidencing little or no deliberation.”

*United States v. Black*, 995 F.2d 233, 1993 WL 181388 (9th Cir. 1993) (unpublished)

The defendant was convicted of aiding and abetting the violation of 18 U.S.C. § 245(b)(2)(F), in violation of 18 U.S.C. § 2, after he approached an African American man near a convenience store and gasoline station, uttered racial slurs, forced him toward the street, and then stabbed the victim several times. On appeal, the defendant argued that there was insufficient evidence to support his conviction because the government did not prove that he intended to deprive the victim of the use of a public facility. The court disagreed, citing the testimony of four witnesses and a note from the defendant to another inmate in prison, which all indicated that the defendant attacked the victim because he was African American and because he was in the defendant’s neighborhood. The court held that this evidence was sufficient for a rational jury to infer that the defendant intended to deprive the victim of the use of the convenience store and gasoline station.

*United States v. McInnis*, 976 F.2d 1226 (9th Cir. 1992)

The defendant was convicted of violating 42 U.S.C. § 3631 after he twice fired a single-action rifle into the home of an African American family, who lived next door. The shots pierced two walls and struck one occupant’s stomach, requiring surgery. The defendant appealed, claiming that the evidence was insufficient to prove that he had the specific intent to injure, intimidate, or interfere with the victim because of her race and because of the victim’s occupation of her home. The court rejected this argument based on the defendant’s numerous racial remarks immediately before the shooting. Furthermore, the police found numerous items of racist paraphernalia in the defendant’s home. The defendant challenged the admission into evidence of these items as unduly prejudicial because each bore swastikas, but the court rejected the argument. The court also accepted the government’s argument that the district court improperly sentenced the defendant

by failing to correctly calculate the base offense level using assault as the underlying crime.

*United States v. Skillman*, 922 F.2d 1370 (9th Cir. 1990)

The defendant was convicted of violating 18 U.S.C. § 241, 42 U.S.C. § 3631(a), and other statutes after burning a cross outside the home of an African American family. On appeal, the defendant claimed there was insufficient evidence to convict him because he was merely present at the scene of the crime. The court, however, held that the requisite “slight connection” existed in that the defendant carried a can of gasoline to the scene of the crime. The court also rejected the defendant’s contention that he was unduly prejudiced by discussion of his status as a skinhead at trial; the evidence was deemed relevant, given that the racial implications were part of the elements of the § 3631 charge. The court also upheld the application of a vulnerable victim sentencing enhancement, reasoning that the defendant “knew or should have known that a black family . . . would be terrified and particularly susceptible to this criminal conduct.”

*United States v. Gilbert*, 884 F. 2d 454 (9th Cir. 1989), overruled by *United States v. Hanna*, 293 F.3d 1080 (9th Cir. 2002)

The defendant was convicted of violating 42 U.S.C. § 3631 for interfering with the adoptive placement of African American children in homes. The defendant appealed, arguing that his racist letters to an adoption agency were not threatening, but instead were political discussions. The court held that the jury could find that there were threats in the letter, especially given that the defendant was a leader of an extremist hate group and that, per § 3631, the threats were intentionally made.

*United States v. Gilbert*, 813 F.2d 1523 (9th Cir. 1987)

The district court dismissed with prejudice an indictment charging defendant with violating 42 U.S.C. § 3631 for failing to state an offense after the defendant mailed racially derogatory and threatening correspondence to the director of an adoption agency that placed African-American and Asian children in homes. The district court reasoned that “adoption efforts focus on placement of a child with a family and not on placement of a child in a dwelling.” On appeal, the government argued that the district court construed too narrowly the definitions of dwelling and occupation. The court of appeals sided with the government, finding that both dwelling and occupation had traditionally been accorded a broad interpretation. “[I]t is unnecessary for a dwelling to be in existence or occupied. A prospective dwelling is sufficient. Second, the occupation of a dwelling does not need to be permanent or associated with property rights . . . Applying these principles here, we hold that the placement of minority children by the director of an adoption agency is a protected activity . . . since the director is ‘aiding or encouraging’ minorities in the occupancy of dwellings . . . The relationship between an adoption agency and the occupancy of a dwelling is not ‘too remote.’”

*United States v. Henery*, 60 F. Supp. 3d 1126 (D. Idaho 2014)

The defendant was charged with violating 18 U.S.C. § 249(a)(1) for attacking an African American man at a club while yelling gang calls and racial slurs. The district court upheld Congress’s authority under the Thirteenth Amendment to enact § 249(a)(1).

*United States v. Gardner*, 993 F. Supp. 2d 1294 (D. Or. 2014)

The defendant was charged with violating the Victim and Witness Protection Act for misleading police officers about a federal hate crime. The defendant argued that the hate crime (18 U.S.C. § 249(a)(2)) underlying her substantive offense was an unconstitutional exercise of Congress’s Commerce Clause authority and that, for that reason, her substantive charge should likewise be dismissed. The district court held that § 249(a)(2) was a constitutional exercise of Congress’s Commerce Clause authority.

*United States v. Mason*, 993 F. Supp. 2d 1308 (D. Or. 2014)

The defendant was charged with violating 18 U.S.C. § 249(a)(2) for assaulting a man because of his sexual orientation. The district court held that § 249(a)(2) was a constitutional exercise of Congress’s Commerce Clause authority.

*United States v. Crawford*, 66 F. Supp. 3d 1311 (D. Or. 2014)

The defendant was charged with violating 18 U.S.C. § 247(c) for setting fire to a mosque. The district court admitted defendant’s anti-Muslim statements into evidence over objection that such evidence was impermissible “propensity” evidence. The court found that the evidence was “offered for a permissible purpose and not simply to show propensity,” and noted that the government was required under the statute to prove that the defendant set fire to the mosque because of

his feelings about Muslims. For this reason, the court explained, the government sought “to admit defendant’s comments to show his intent and state of mind—not his propensity to commit arson or damage religious property generally.”

*United States v. Furrow*, 125 F. Supp. 2d 1178 (C.D. Cal. 2000)

The defendant filed a motion to dismiss the indictment charging him with violating 18 U.S.C. §§ 245(b)(2)(F) and (b)(4)(A), arguing that the statute was unconstitutional. The district court held that Congress validly enacted § 245 pursuant to its Commerce Clause authority.

### **Tenth Circuit**

*United States v. Hatch*, 722 F.3d 1193 (10th Cir. 2013)

The defendant pled guilty to violating 18 U.S.C. § 249(a)(1) after kidnapping a disabled Native American man and burning a swastika into his arm. The court of appeals upheld the constitutionality of 18 U.S.C. § 249(a)(1) as a valid exercise of Congress’s Thirteenth Amendment authority.

*United States v. Egbert*, 562 F.3d 1092 (10th Cir. 2009)

The defendants, members of a white supremacist organization, were convicted of violating 18 U.S.C. § 241 and 18 U.S.C. § 245(b)(2)(C) after they assaulted, while uttering racist slurs, a Mexican American bartender who had asked them to leave the bar after other patrons complained that they had distributed white supremacist literature. A few months later, one of the defendants, along with other white supremacists, lured three men, one of whom they suspected to be Native American, from a bar and then beat one of the victims until he stopped moving. The defendants did not challenge their convictions, but successfully argued on appeal that they were entitled to a sentence reduction because (1) the evidence did not support a finding that the victim suffered serious bodily injury, and (2) one of the defendants had not played a leadership role in the offense.

*United States v. Magleby*, 420 F.3d 1136 (10th Cir. 2005) (affirming denial of habeas relief) and *United States v. Magleby*, 241 F.3d 1306 (10th Cir. 2001) (affirming convictions)

The defendant was convicted of violating 18 U.S.C. § 241, 42 U.S.C. § 3631, and other statutes after he burned a cross on the lawn of an interracial family’s home. The court of appeals rejected his argument that there was insufficient evidence for a conviction. The court rejected the defendant’s argument that the jury instructions were flawed in that they would allow the jury to convict him based on the fact that one of the victims was black, but without finding that the defendant was motivated based on the victims’ occupation of their home. The court also held that there was no error in instructing the jury that it could consider the reaction of the victims in determining the defendant’s intent. The court questioned the government’s use of an expert on hate groups and an avowed racist who knew the defendant, but held any error in doing so was harmless. The court permitted the introduction of racist song lyrics the defendant listened to shortly before the crime. On appeal from a denial of habeas corpus relief, the court agreed that the § 241 instruction was flawed because it never defined “threat” as “requiring a threat of force.” “Many acts short of unlawful violence may constitute oppression or intimidation in the everyday sense of these words.” Nevertheless, the court did not find it objectively unreasonable for appellate counsel not to raise this challenge.

*United States v. Grassie*, 237 F.3d 1199 (10th Cir. 2001)

The defendant was convicted of violating 18 U.S.C. § 247 after burning one church and defacing and damaging four others. The court of appeals rejected defendant’s challenge to the constitutionality of § 247, holding that the evidence at trial showed “the extensive use of these church buildings for a broad range of religious, cultural, social, recreational, welfare, educational, and financial activities.” In addition, the defendant had stipulated that the churches were “engaging in activities affecting interstate commerce.” The court also upheld the district court’s jury instruction that a finding of “any effect at all on interstate commerce” was enough to satisfy a statutory element, and alternatively ruled that the jury “necessarily made its decision in light of an unqualified ‘affecting commerce’ stipulation.” The court also rejected the defendant’s argument that his convictions under both §§ 247 and 844(h)(1) (use of a fire to commit a felony) violated Double Jeopardy.

*United States v. Whitney*, 229 F.3d 1296 (10th Cir. 2000)

The defendants were convicted of violating 18 U.S.C. § 241 and 42 U.S.C. § 3631 after burning a cross on the lawn of an African American family’s home. The court of appeals found the evidence sufficient to sustain both convictions.

*United States v. Woodlee*, 136 F.3d 1399 (10th Cir. 1998)

The defendants were convicted of violating 18 U.S.C. § 245(b)(2)(F) after making racial comments and threats toward African American men in a bar, following them from the bar, following them in a high speed car chase, and then firing a rifle into the victims' car, hitting one of the victims. On appeal, the defendants argued that the government needed to show that they had intended to injure a victim rather than merely intimidate or interfere with a right in a manner that resulted in injury. The court disagreed, holding that § 245(b) expressly provides that the government need only show that the defendant's illegal conduct resulted in bodily injury; the standard is one of causation, not state of mind. One defendant also challenged the admission of witness testimony, under Fed. R. Evid. 404(b), regarding his racist attitudes. The court disagreed, explaining that under § 245(b)(2)(F), the government was required to prove that the defendant had acted because of the victims' race. The court held that evidence of past racial animosity was relevant to establish this element of the offense, and therefore, it fell squarely within the motive and intent purposes delineated in 404(b).

*United States v. Lane*, 883 F.2d 1484 (10th Cir. 1989)

The defendants, who had participated in the formation of an anti-Semitic group known as the Order, were convicted of violating 18 U.S.C. § 245(b)(2)(C) after shooting and killing a Jewish radio talk-show host who had criticized the Ku Klux Klan on his show. The court of appeals rejected defendants' argument that § 245(b)(2)(C) was unconstitutional, and held that Congress validly enacted the statute pursuant to its Commerce Clause authority. Defendants also argued that there was insufficient evidence to establish that their participation in the victim's murder was motivated by the fact that the victim had been enjoying employment or any prerequisite thereof. The court disagreed, holding that the government had introduced sufficient evidence from which a rational jury could have found beyond a reasonable doubt that, among other things, the victim came to defendants' attention because of his employment as a radio talk-show host and his comments criticizing right-wing extremist groups.

*United States v. Franklin*, 704 F.2d 1183 (10th Cir. 1983)

The defendant was convicted of violating 18 U.S.C. § 245(b)(2)(B) after he shot and killed two black men who had been jogging with white women at a public park. The defendant argued on appeal that there was insufficient evidence to support his conviction, suggesting that the government had failed to establish that the black victims had been killed because they had been enjoying a public facility. The court disagreed, stating that several witnesses had testified that the defendant had disapproved of racial mixing at the public park; specifically, two witnesses testified that the defendant had told them he had shot two black joggers "to do something about it." The court found that the jury could have inferred that the defendant intended to deprive the victims of the opportunity to enjoy public parks.

*United States v. Beebe*, 807 F. Supp. 2d 1045 (D.N.M. 2011)

Defendants were charged with violating 18 U.S.C. § 249(a)(1) after kidnapping a disabled Native American man and burning a swastika into his arm. The district court upheld the constitutionality of 18 U.S.C. § 249(a)(1) as a valid exercise of Congress's Thirteenth Amendment authority. The defendants had argued that it was irrational for Congress to determine that physical violence was a badge and incident of slavery. The district court, after a review of history, held "[a] cursory review of the history of slavery in America demonstrates that Congress's conclusion is not merely rational, but inescapable."

## **Eleventh Circuit**

*United States v. Ballinger*, 395 F.3d 1218 (11th Cir. 2005) (en banc)

The defendant was convicted of violating 18 U.S.C. § 247 after burning several churches in several states. The en banc court upheld the constitutionality of § 247, holding that it was a valid exercise of Congress's Commerce Clause authority to regulate the channels and instrumentalities of interstate commerce. The court also held that § 247 applied to the defendant's conduct, reasoning that if "§ 247's prohibition on destroying religious property in commerce does not reach [the defendant's] four-state church-arson spree, there is implausibly little, if any, conduct it actually proscribes." Given this finding, the court did not address whether the defendant's conduct *affected* interstate commerce.

*United States v. Odom*, 252 F.3d 1289 (11th Cir. 2001)

Defendants were convicted of various offenses in connection with a church arson. In reversing their 18 U.S.C. § 844(i) conviction, the court of appeals held that the church was not sufficiently used in interstate commerce. Evidence of a church's relationship to interstate commerce must establish that this relationship relates to its "business" as a church. Even

activities that more closely resemble commerce—such as the purchase of hymnals—do not necessarily constitute the “requisite nexus” between the building’s function and interstate commerce. Here, materials for the church and its Sunday School had been purchased across state lines, gas purchased in Alabama—where the church is located—was originally from Mississippi, and the church paid dues for its membership in an intrastate church association that sent delegates to a national convention. No evidence indicated that the church here had been selected to attend the national convention or that an interstate traveler had visited the church. These activities did not establish the “requisite nexus” because they were “too passive, too minimal, and too indirect.”

*United States v. Stewart*, 65 F.3d 918 (11th Cir. 1995)

The defendants, KKK members, were convicted of violating 18 U.S.C. § 241, 42 U.S.C. § 3631, and 18 U.S.C. § 844(h)(1) after they burned a cross in the yard of the first African American family to live in a “virtually all-white community.” The appeal primarily concerned the district court’s *Batson* process, but defendants also argued that they had been convicted of three counts involving the same conduct—burning a cross—in violation of the Double Jeopardy Clause. “The Double Jeopardy Clause does not bar cumulative punishments stemming from a single incident when Congress intends to prescribe cumulative punishments.” The court found clear legislative intent to allow multiple punishments. The Court also found that the statutes were facially valid and not unconstitutional as applied. “Notwithstanding the fact that some Klan cross-burnings may constitute protected expression, these defendants did not burn their cross simply to make a political statement.”

*United States v. Long*, 935 F.2d 1207 (11th Cir. 1991)

After being charged with violating 18 U.S.C. § 241, 42 U.S.C. § 3631, and 18 U.S.C. § 844(h)(1) for having constructed a cross and burned it on the front lawn of an African American family that moved into a rural white neighborhood, the defendants pleaded guilty to violating § 241. They appealed various sentencing issues, many propositions of which are no longer good law due to changes in the Guidelines. *See United States v. Yount*, 960 F.2d 955 (11th Cir. 1992) (“The current version [of the Sentencing Guidelines] appears to require that the victim of the offense must have been unusually vulnerable and specifically targeted in the offense.”).

*United States v. Worthy*, 915 F.2d 1514 (11th Cir. 1990)

Defendants pled guilty to violating 18 U.S.C. § 241 for their involvement in a cross-burning at the residence of a black family and stipulated that they burned the cross to intimidate the family. On appeal, the court held that burning a cross constitutes the use of fire in the commission of a felony for purposes of applying the Sentencing Guidelines.

*United States v. White*, 846 F.2d 678 (11th Cir. 1988)

The defendant, a member of the Ku Klux Klan who allegedly clashed with black marchers led by the Southern Christian Leadership Conference (SCLC), was charged with conspiracy to violate 18 U.S.C. § 245(b)(2)(B). The district court granted the defendant’s motion for judgment of acquittal, finding that the government had failed to prove that the parade was “provided or administered by” the city within the meaning of § 245(b)(2)(B). The court of appeals reversed, holding that protestors who lack a parade permit are not outside the coverage of § 245(b)(2)(B), and that the city “administered” the parade and “provided” the police protection and the streets on which the parade occurred. The court also concluded that, based on the legislative history of § 245, racially-motivated violence during parades, marches, and demonstrations was precisely what § 245 was designed to redress.

*United States v. Wood*, 780 F.2d 955 (11th Cir. 1986)

The defendants, KKK members, were convicted of violating 18 U.S.C. § 241 and 42 U.S.C. § 3631 after they broke into a home while armed with guns, ransacked it, and beat its occupants because they were in an interracial relationship. On appeal, the defendants argued that they had no intent to force the victim to move. The court responded: “The distinction which they seek to draw between conduct designed to force a victim to move from his home (such as firebombing or a direct order to leave) and actions intended to intimidate the occupant into giving up a federally protected right to associate in his home with members of another race as a condition of safe occupancy is without merit.”

## **D.C. Circuit**

*United States v. Syring*, 522 F. Supp. 2d 125 (D.D.C. 2007)

The defendant was charged with violating 18 U.S.C. § 245 (b)(2)(C) for sending threatening voicemail and email messages to employees of the Arab American Institute. Before trial, the defendant moved to dismiss the indictment,

arguing that § 245 violated his First Amendment rights by criminalizing protected speech. The district court rejected the defendant's claim, explaining that the First Amendment does not protect "true threats," that whether a statement is a true threat is a jury question, and that a reasonable jury could conclude that defendant's communications amounted to a true threat.

## Note from the Editor . . .

We are pleased to bring this Bulletin to you concerning emerging issues in the practice of the United States Attorney community and the Department family. Our sincere thanks to Gretchen Shappert. Gretchen served as the coordinating editor on this issue by selecting the topics, recruiting the authors, and reviewing the articles. Her work made this issue possible. During her time in EOUSA, Gretchen was the driving force behind many of the Bulletin issues. Her dedication and hard worked resulted in several top quality issues you have enjoyed over the past few years. Gretchen is presently serving as the United States Attorney in the Virgin Islands. We wish her well in her new role, although here at the Bulletin, we will miss her tremendously.

We are excited about our schedule of issues for this year. Issues on bankruptcy, training, opioids, cyber-crime, Project Safe Neighborhood, corporate crime, appeals, and the rule of law are scheduled and in the works. If you have a suggestion for a Bulletin topic or if you are interested in authoring an article, please contact me at [tate.chambers@usdoj.gov](mailto:tate.chambers@usdoj.gov). Thank you for your continued readership.

Thank you,

K. Tate Chambers

2017

# Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web

Ahmed Ghappour

Follow this and additional works at: [https://repository.uchastings.edu/faculty\\_scholarship](https://repository.uchastings.edu/faculty_scholarship)

---

## Recommended Citation

Ahmed Ghappour *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web* 69 *Stan. L. Rev.* 1075 (2017).  
Available at: [https://repository.uchastings.edu/faculty\\_scholarship/1583](https://repository.uchastings.edu/faculty_scholarship/1583)



## ARTICLE

## Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web

Ahmed Ghappour\*

**Abstract.** The use of hacking tools by law enforcement to pursue criminal suspects who have anonymized their communications on the dark web presents a looming flashpoint between criminal procedure and international law. Criminal actors who use the dark web (for instance, to commit crimes or to evade authorities) obscure digital footprints left behind with third parties, rendering existing surveillance methods obsolete. In response, law enforcement has implemented hacking techniques that deploy surveillance software over the Internet to directly access and control criminals' devices. The practical reality of the underlying technologies makes it inevitable that foreign-located computers will be subject to remote "searches" and "seizures." The result may well be the greatest extraterritorial expansion of enforcement jurisdiction in U.S. law enforcement history.

This Article examines how the government's use of hacking tools on the dark web profoundly disrupts the legal architecture on which cross-border criminal investigations rest. These overseas cyberoperations raise increasingly difficult questions regarding who may authorize these activities, where they may be deployed, and against whom they may lawfully be executed. The rules of criminal procedure fail to regulate law enforcement hacking because they allow these critical decisions to be made by rank-and-file officials despite potentially disruptive foreign relations implications. This Article outlines a regulatory framework that reallocates decisionmaking to the institutional actors who are best suited to determine U.S. foreign policy and avoids sacrificing law enforcement's ability to identify and locate criminal suspects who have taken cover on the dark web.

---

\* Visiting Assistant Professor, U.C. Hastings College of the Law. For helpful conversations, comments, and support, I thank Ryan Calo, Anupam Chander, Bobby Chesney, Danielle Citron, Jennifer Daskal, Bill Dodge, Scott Dodson, Derek Jinks, Elizabeth Joh, Orin Kerr, Rick Marcus, Tara Mikkilineni, Paul Ohm, Austen Parrish, Stephanie K. Pell, Morris Ratner, Bertrall Ross, Reuel Schiller, Chris Soghoian, David Sloss, and Katherine Strandburg. I also thank participants in workshops and conferences at American University Washington College of Law, U.C. Berkeley School of Law, U.C. Davis School of Law, U.C. Hastings College of the Law, N.Y.U. School of Law, the U.S. Military Academy, and Yale Law School for their helpful comments and conversations. Finally, I thank the editors of the *Stanford Law Review* for their terrific editing.

**Table of Contents**

Introduction.....1077

I. Law Enforcement in the Dark.....1087

    A. The Dark Web.....1087

    B. Failure of Conventional Surveillance Methods.....1090

    C. Hacking as an Investigative Tool on the Dark Web.....1095

II. Law Enforcement out of Bounds.....1099

    A. Conventional Methods Are in Harmony with International Law.....1099

    B. Failure of the Existing Rules.....1106

    C. The Foreign Relations Risk of Hacking the Dark Web.....1108

        1. The risk of attribution.....1108

        2. The risk of vulnerability disclosure.....1110

        3. The risk to diplomatic legitimacy.....1112

        4. The risk of foreign prosecution.....1115

        5. The risk of countermeasures.....1116

III. Toward a Normative Legal Process.....1122

    A. Failure of the Existing Legal Process.....1123

    B. Substantive Policy Preferences.....1128

        1. What hacking techniques should be authorized?.....1128

        2. Who should be targeted?.....1130

        3. What crimes should trigger use of hacking techniques?.....1130

    C. Implementation and Enforcement.....1132

Conclusion.....1135

## Introduction

Nestled deep beneath the surface of the World Wide Web, Dread Pirate Roberts (DPR) ran an underground empire of criminality. Not much was known about DPR, except that he appeared to have built the Silk Road—a global online marketplace for illicit services and contraband.<sup>1</sup> DPR—later identified as Ross Ulbricht—was the target of a global manhunt that operated in the dark for nearly three years.<sup>2</sup> In that time, the Silk Road attracted over 100,000 users who transacted over one million deals, generating an estimated \$1.2 billion in global sales from vendors located in more than ten countries around the world.<sup>3</sup>

The Silk Road was built to facilitate black market transactions. It was hosted on the dark web, a global network of computers that use a cryptographic protocol to communicate, enabling users to conduct transactions anonymously without revealing their location.<sup>4</sup> Users could only make payments in the digital currency Bitcoin, and transactions were run through a “series of dummy transaction[s] to disguise the link between buyers and

- 
1. MARC GOODMAN, *FUTURE CRIMES: EVERYTHING IS CONNECTED, EVERYONE IS VULNERABLE, AND WHAT WE CAN DO ABOUT IT* 194 (2015); Press Release, U.S. Att’y’s Office for the S. Dist. of N.Y., U.S. Dep’t of Justice, Ross Ulbricht, A/K/A “Dread Pirate Roberts,” Sentenced in Manhattan Federal Court to Life in Prison (May 29, 2015), <https://www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison>.
  2. The Silk Road website went live in February 2011. See GOODMAN, *supra* note 1, at 198. U.S. agencies commenced a number of independent Silk Road investigations in the fall of 2011. See, e.g., Transcript of Trial at 1389, *United States v. Ulbricht*, No. 14 Cr. 68 (KBF) (S.D.N.Y. Jan. 28, 2015) (relating a joint stipulation by the government and defense that if called to testify, Special Agent Richardson of the Drug Enforcement Administration would testify that she attempted a number of purchases on the Silk Road website between September 2011 and May 2013 as part of an undercover investigation); Transcript of Trial at 71, 153, *Ulbricht*, No. 14 Cr. 68 (KBF) (S.D.N.Y. Jan. 14, 2015) (indicating via in-court testimony that the U.S. Department of Homeland Security (DHS) commenced its investigation in October 2011); Affidavit of Special Agent Ilhwan Yum in Support of a Search Warrant at 1, 6, *United States v. Certain Premises*, No. 13-1051-M (E.D. Pa. Sept. 9, 2013) (stating that an investigation by the Federal Bureau of Investigation (FBI) was ongoing as of November 2011). Ulbricht was arrested on October 1, 2013. See Affidavit of Special Agent Tigran Gambaryan in Support of Criminal Complaint at 11, *United States v. Force*, No. 3-15-70370 (N.D. Cal. Mar. 25, 2015). The Silk Road was shuttered by the FBI on October 2, 2013. See *id.* at 10.
  3. See Press Release, U.S. Att’y’s Office for the S. Dist. of N.Y., *supra* note 1; see also Donna Leinwand Leger, *How FBI Brought Down Cyber-Underworld Site Silk Road*, USA TODAY (May 15, 2014, 2:54 PM EDT), <http://usat.ly/1b8Gntk> (“Beyond illegal drugs, the site served as a bazaar for fake passports, driver’s licenses and other documents, as well as illegal service providers, such as hit men, forgers and computer hackers.”).
  4. Leger, *supra* note 3. To access the Silk Road, users needed specialized anonymity software allowing them to communicate on the dark web. *Id.*

sellers.<sup>5</sup> Thousands of drug dealers flocked to the Silk Road because of the anonymity it promised;<sup>6</sup> there, they conducted over a million drug deals out of reach of law enforcement's most advanced electronic surveillance tools.<sup>7</sup>

Investigators made bold efforts to infiltrate the hidden website to identify DPR. They posed as buyers and sellers on the site, completing over a hundred purchases.<sup>8</sup> One agent even infiltrated the staff of the website, spending ten to twelve hours per day administering the site and communicating with DPR directly.<sup>9</sup> All for naught. Their attempts failed because existing surveillance methods rely on digital trails left behind with third parties by computers on the web—the very information obscured by the dark web. In the end, it was an IRS agent who solved the case, stumbling upon communications on a public website advertising the Silk Road just before its launch in 2011.<sup>10</sup> Because of Ulbricht's own human error, the communication was traced back to him,<sup>11</sup> and the alleged kingpin was apprehended, prosecuted, and sentenced to life in prison.<sup>12</sup>

Several underground marketplaces surfaced in the wake of the Silk Road,<sup>13</sup> highlighting an asymmetry between investigators' ability to track unlawful activity and criminals' capacity to commit crimes on the dark web.<sup>14</sup> The

---

5. *Id.*

6. See Transcript of Trial at 42, *Ulbricht*, No. 14 Cr. 68 (KBF) (S.D.N.Y. Jan. 13, 2015) (“Thousands of drug dealers flocked to Silk Road, and more than 1 million drug deals took place on the site before the government shut it down.”).

7. See *id.*; Leslie R. Caldwell, *Ensuring Tech-Savvy Criminals Do Not Have Immunity from Investigation*, U.S. DEPT JUST. BLOGS (Nov. 21, 2016), <https://www.justice.gov/opa/blog/ensuring-tech-savvy-criminals-do-not-have-immunity-investigation> (“[T]he abuse of internet anonymizing technology . . . [is] the digital equivalent of crimes committed in the middle of a busy street, in full view of the citizenry and the police, with little risk of being caught.” (italics omitted)).

8. See GOODMAN, *supra* note 1, at 196.

9. See Andy Greenberg, *Undercover Agent Reveals How He Helped the FBI Trap Silk Road's Ross Ulbricht*, WIRED (Jan. 14, 2015, 6:34 PM), <https://www.wired.com/2015/01/silk-road-trial-undercover-dhs-fbi-trap-ross-ulbricht>.

10. See Nathaniel Popper, *The Tax Sleuth Who Took Down a Drug Lord*, N.Y. TIMES: DEALBOOK (Dec. 25, 2015), <http://nyti.ms/1R02DMZ>.

11. See *id.*

12. See Transcript of Sentencing at 94, *Ulbricht*, No. 14 Cr. 68 (KBF) (S.D.N.Y. May 29, 2015). In the interest of disclosure, the Author advised on Ulbricht's appeal.

13. See, e.g., Steven Nelson, *Buying Drugs Online Remains Easy, 2 Years After FBI Killed Silk Road*, U.S. NEWS & WORLD REP. (Oct. 2, 2015, 3:12 PM), <http://www.usnews.com/news/articles/2015/10/02/buying-drugs-online-remains-easy-2-years-after-fbi-killed-silk-road>; Benjamin Weiser, *Man Charged with Operating Silk Road 2.0, a Black Market Website*, N.Y. TIMES (Nov. 6, 2014), <http://nyti.ms/1slvgVH>.

14. For example, Senator Tom Carper (D-Del.), then-Chairman of the Senate Homeland Security and Governmental Affairs Committee, stated at the time of the launch of Silk Road 2.0: “This new website—launched barely a month after Federal agents shut down  
*footnote continued on next page*

existence of hidden services like the Silk Road “dramatically lower[s] the entry barriers into the underground economy—for both buyers and sellers” of illicit goods and services.<sup>15</sup> The use of the dark web by criminal actors therefore enables secret, untraceable criminal activity to take place at scale. This has led policymakers to question whether law enforcement has sufficient tools to counter the illicit conduct that might flow through the digital underworld.<sup>16</sup>

The term “network investigative technique” is a euphemism for law enforcement hacking; it describes a law enforcement surveillance method that entails remotely accessing and installing malware on a computer without the permission of its owner or operator.<sup>17</sup> Network investigative techniques are especially useful in the pursuit of criminal suspects who use anonymizing software to obscure their location. By accessing the target computer directly and converting it into a surveillance device, use of network investigative techniques circumvents the need to know a target’s location and makes the

---

the original Silk Road—underscores the inescapable reality that technology is dynamic and ever-evolving and that government policy needs to adapt accordingly.” Press Release, Sen. Tom Carper, Chairman, Senate Homeland Sec. & Governmental Affairs Comm., Chairman Carper Statement on the Unveiling of the So-Called “Silk Road 2.0” Website (Nov. 6 2013), <https://www.hsgac.senate.gov/media/majority-media/chairman-carper-statement-on-the-unveiling-of-the-so-called-silk-road-20-website>.

15. See Government Sentencing Submission at 2, *Ulbricht*, No. 14 Cr. 68 (KBF) (S.D.N.Y. May 26, 2015).
16. See, e.g., Press Release, Sen. Tom Carper, *supra* note 14.
17. This Article uses the terms “network investigative technique,” “cyberexfiltration operation,” and “hacking” interchangeably to describe the use of software that subverts a computer. In computer science, the common term is “malware” (short for “malicious software”). See ROBERT SLADE, *DICTIONARY OF INFORMATION SECURITY* 118 (2006) (defining malware as a “collective term including the many varieties of deliberately malicious software; that is, software written for the purpose of causing inconvenience, destruction, or the breaking of security policies or provisions”). Law enforcement has used a wide variety of other terms to refer to hacking, including “Computer and Internet Protocol Address Verifier” (CIPAV), “Internet Protocol Address Verifier” (IPAV), “Remote Access Search and Surveillance” (RASS), “Remote Computer Search,” “Remote Search,” “Computer Tracer,” “Internet Tracer,” “Remote Computer Trace,” and “Web Bug.” See, e.g., Application & Affidavit of Special Agent Norman B. Sanders, Jr. for Search Warrant at 2-3, *In re* Search of Any Comput. Accessing Elec. Messages Directed to MySpace Account “Timberlinebombinfo,” No. MJ07-5114 (W.D. Wash. June 12, 2007) [hereinafter Sanders Affidavit] (using “CIPAV”); see also Elec. Frontier Found., FBI CIPAV-8 (n.d.), [https://www.eff.org/files/filenode/cipav/fbi\\_cipav-08.pdf](https://www.eff.org/files/filenode/cipav/fbi_cipav-08.pdf) (consisting of a cache of documents released from the FBI to the Electronic Frontier Foundation showing usage of the terms “CIPAV,” “IPAV,” “RASS,” and “Web Bug” in various FBI correspondences and field office requests for technical assistance from the FBI’s Cryptologic and Electronic Analysis Unit); Elec. Frontier Found., FBI CIPAV-10 (n.d.), [https://www.eff.org/files/filenode/cipav/FBI\\_CIPAV-10.pdf](https://www.eff.org/files/filenode/cipav/FBI_CIPAV-10.pdf) (consisting of a cache of documents released from the FBI to the Electronic Frontier Foundation showing usage of these terms in various FBI field office requests for technical assistance from the FBI’s Cryptologic and Electronic Analysis Unit).

new surveillance method a practical solution for the pursuit of criminal suspects on the dark web. Once installed, the right malware can cause a computer to perform any task the computer is capable of performing.<sup>18</sup> Malware can force the target computer to covertly upload files to a server controlled by law enforcement or instruct the computer's camera or microphone to gather images and sound.<sup>19</sup> It can even commandeer computers that associate with the target by, for example, accessing a website it hosts.<sup>20</sup>

The legal process for the use of network investigative techniques is governed by Federal Rule of Criminal Procedure 41, which articulates procedures for obtaining a search warrant in federal magistrate court. The former version of Rule 41 restricted authority to issue search warrants to the district of the magistrate making the decision.<sup>21</sup> This had caused courts to deny search warrants for computers whose locations were unknown because they may have been outside the magistrate's district.<sup>22</sup> An amendment to the rule laid to rest this administrative hurdle by explicitly permitting magistrates to issue a search warrant for a device if the device's location "has been concealed through technological means."<sup>23</sup> The relevant portion of Rule 41(b)(6) reads:

- 
18. See *What Is Malware?*, PALO ALTO NETWORKS, <https://www.paloaltonetworks.com/documentation/glossary/what-is-malware> (last visited Apr. 4, 2017) (defining "malware" as "a file or code, typically delivered over a network[,] that infects, explores, steals or conducts virtually any behavior an attacker wants"); see also Steven M. Bellovin et al., *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 NW. J. TECH. & INTELL. PROP. 1, 26-27 (2014) (providing a brief technical explanation of how malware can control devices and components of a computer by modifying programs known as "device drivers"); Craig Timberg & Ellen Nakashima, *FBI's Search for 'Mo,' Suspect in Bomb Threats, Highlights Use of Malware for Surveillance*, WASH. POST (Dec. 6, 2013), <https://wpo.st/dooc2> (describing the functionality of various types of malware known to have been used by the FBI).
  19. See *In re Warrant to Search a Target Comput. at Premises Unknown*, 958 F. Supp. 2d 753, 755 (S.D. Tex. 2013) (rejecting an application for a warrant to deploy malware "designed not only to extract certain stored electronic records but also to generate user photographs and location information over a 30 day period"); Timberg & Nakashima, *supra* note 18 (describing malware that turns on a computer's camera); Kim Zetter, *So . . . Now the Government Wants to Hack Cybercrime Victims*, WIRED (May 4, 2016, 7:00 AM), <https://www.wired.com/2016/05/now-government-wants-hack-cybercrime-victims> (describing malware that turns on a computer's microphone).
  20. See Kevin Poulsen, *Visit the Wrong Website, and the FBI Could End Up in Your Computer*, WIRED (Aug. 5, 2014, 6:30 AM), [http://www.wired.com/2014/08/operation\\_torpedo](http://www.wired.com/2014/08/operation_torpedo).
  21. See FED. R. CRIM. P. 41(b)(1)-(5). Rule 41 provides that a search warrant may be issued by "a magistrate judge with authority in the district." See *id.* 41(b).
  22. See, e.g., *In re Warrant to Search a Target Comput. at Premises Unknown*, 958 F. Supp. 2d at 757, 761.
  23. See Letters from Chief Justice John G. Roberts to Paul D. Ryan, Speaker, U.S. House of Representatives, and Joseph R. Biden, Jr., President, U.S. Senate, attachment at 6 (Apr. 28, 2016), [https://www.supremecourt.gov/orders/courtorders/frcr16\\_mj80.pdf](https://www.supremecourt.gov/orders/courtorders/frcr16_mj80.pdf) (submitting amendments to the Federal Rules of Criminal Procedure).

[A] magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located *within or outside* that district if:

(A) the district where the media or information is located has been concealed through technological means . . . .<sup>24</sup>

Although the U.S. Department of Justice (DOJ), in recommending the amendment to Rule 41, explicitly stated that the amendment is not meant to give courts the power to issue warrants that authorize searches in foreign countries,<sup>25</sup> the practical reality of the underlying technology means overseas searches will be both unavoidable and frequent. The result may well be the largest expansion of extraterritorial enforcement jurisdiction in FBI history.<sup>26</sup>

The legal process for network investigative techniques presumes search targets are territorially located, which is not at all accurate. Indeed, most potential targets on the dark web are *outside* the territorial United States.<sup>27</sup> Approximately 80% of the computers on the dark web are located outside the United States.<sup>28</sup> And because each device's location is indistinguishable from that of the next, any given law enforcement target is likely to be located

---

24. FED. R. CRIM. P. 41(b)(6) (emphasis added). The amendment became effective on December 1, 2016. See *id.* advisory committee's note to 2016 amendment.

25. See Letter from Mythili Raman, Acting Assistant Att'y Gen., Criminal Div., U.S. Dep't of Justice, to Judge Reena Raggi, Chair, Advisory Comm. on Rules of Criminal Procedure 4 (Sept. 18, 2013), in ADVISORY COMM. ON CRIMINAL RULES, ADVISORY COMMITTEE ON RULES OF CRIMINAL PROCEDURE: APRIL 2014, at 171, 174 (2014), [http://www.uscourts.gov/sites/default/files/fr\\_import/CR2014-04.pdf](http://www.uscourts.gov/sites/default/files/fr_import/CR2014-04.pdf).

26. See Ahmed Ghappour, *Justice Department Proposal Would Massively Expand FBI Extraterritorial Surveillance*, JUST SECURITY (Sept. 16, 2014, 9:10 AM), <http://justsecurity.org/15018/justice-department-proposal-massive-expand-fbi-extraterritorial-surveillance>.

27. For example, in the Silk Road case, computer security experts who were following or associated with the case opined that it was possible the FBI hacked into Silk Road servers, located in Iceland, to extract key evidence used in the prosecution and forfeiture proceedings. See, e.g., Joseph Cox, *How Did the FBI Find the Silk Road Servers, Anyway?*, MOTHERBOARD (Oct. 3, 2014, 8:55 AM), <http://motherboard.vice.com/read/how-did-the-fbi-find-the-silk-road-servers-anyway>. This issue was raised by the defense and denied on standing grounds and is currently on appeal. See Brief for Defendant-Appellant at 108, United States v. Ulbricht, No. 15-1815-CR (2d Cir. Jan. 12, 2016), 2016 WL 158389; see also Andy Greenberg, *Fed's Silk Road Investigation Broke Privacy Laws, Defendant Tells Court*, WIRED (Aug. 2, 2014, 2:54 PM), <https://www.wired.com/2014/08/feds-silk-road-investigation-violated-privacy-law-sites-alleged-creator-tells-court>. More recently, as part of a child pornography investigation the FBI infected thousands of computers overseas with malware. See Joseph Cox, *FBI Hacked Over 8,000 Computers in 120 Countries Based on One Warrant*, MOTHERBOARD (Nov. 22, 2016, 6:18 PM EST) [hereinafter Cox, *FBI Hack*], <http://motherboard.vice.com/read/fbi-hacked-over-8000-computers-in-120-countries-based-on-one-warrant>.

28. See *Top-10 Countries by Relay Users*, TORMETRICS, <https://metrics.torproject.org/userstats-relay-table.html> (last visited Apr. 4, 2017).

abroad. Thus, the issue is not whether magistrates should be authorized to issue search warrants where the target of the search can be in any of the ninety-four federal judicial districts in the United States. Instead, the issue is whether (and how) investigators should conduct out-of-district searches where targets are likely to be located *out-of-country* as well.

The extraterritorial aspect of law enforcement hacking operations has drawn sharp public criticism by a wide array of commentators, academics, civil liberties organizations, and technology corporations.<sup>29</sup> Technology giant Google warned that the use of network investigative techniques in pursuit of targets on the dark web would undermine the sovereignty of nations by “authorizing the government to conduct searches outside the United States.”<sup>30</sup> Google and others cautioned that loosening territorial restrictions on the government’s search and seizure power “raises a number of monumental and highly complex constitutional, legal, and geopolitical concerns.”<sup>31</sup> While the Advisory Committee on Rules of Criminal Procedure flagged this concern,<sup>32</sup> noting the potential regulatory gap regarding cross-border searches, it explicitly left such “issues that may have foreign policy implications” to be dealt with through “inter-executive branch coordination.”<sup>33</sup>

Whether law enforcement is permitted to launch cross-border cyberexfiltration operations is the latest in a series of questions testing the limits of unilateral investigatory activities in a globally networked world. At the core of the inquiry is the well-established international law axiom that one state may

- 
29. The Rule 41 Subcommittee received more than fifty written comments in addition to comments that were presented at hearings before the full Advisory Committee in November 2014. See *Proposed Amendments to the Federal Rules of Criminal Procedure*, REGULATIONS.GOV, <https://www.regulations.gov/docketBrowser?rpp=25&so=DESC&sb=commentDueDate&po=0&D=USC-RULES-CR-2014-0004> (last visited Apr. 4, 2017). Civil liberties groups that submitted public comments included the ACLU, the Center for Democracy & Technology, the Electronic Frontier Foundation, the Electronic Privacy Information Center, and the National Association of Criminal Defense Lawyers. See *id.*
30. Letter from Richard Salgado, Dir. of Law Enf’t & Info. Sec., Google Inc., to the Advisory Comm. on Rules of Criminal Procedure 2-3 (Feb. 13, 2015), <https://www.regulations.gov/contentStreamer?documentId=USC-RULES-CR-2014-0004-0029&attachmentNumber=1&contentType=pdf>.
31. *Id.* at 1; see also, e.g., Ctr. for Democracy & Tech., Written Statement of the Center for Democracy & Technology Before the Advisory Committee on Rules of Criminal Procedure 4 (2014), <http://www.regulations.gov/#documentDetail;D=USC-RULES-CR-2014-0004-0009> (“Unilateral extraterritorial searches may violate the international obligations of the United States.”).
32. See Memorandum from Sara Sun Beale & Nancy King, Reporters, to Advisory Comm. on Rules of Criminal Procedure 13-14 (Feb. 25, 2015), in ADVISORY COMM. ON CRIMINAL RULES, ADVISORY COMMITTEE ON RULES OF CRIMINAL PROCEDURE: MAY 2015, at 87, 99-100 (2015), [http://www.uscourts.gov/sites/default/files/fr\\_import/CR2015-05.pdf](http://www.uscourts.gov/sites/default/files/fr_import/CR2015-05.pdf).
33. *Id.* at 14-15.

not unilaterally exercise its law enforcement functions in the territory of another state,<sup>34</sup> which has not been adequately addressed by courts or scholarship in the context of cyberspace.

While there is a wealth of scholarship on the relationship between the Internet and state sovereignty, its focus has almost exclusively been on the permissibility of one state's laws regulating Internet conduct that takes place in another state (exercising "prescriptive jurisdiction"), rather than the permissibility of a state effectuating compliance with those laws in the territory of another state (exercising "enforcement jurisdiction").<sup>35</sup> Jack Goldsmith offers perhaps the most sustained focus on the issue of cross-border enforcement jurisdiction. He argues that while multiple nations may in theory regulate the same Internet transaction, the system as a whole is stable in part because each nation can only *enforce* regulations within its territory.<sup>36</sup> Thus, while states may criminalize conduct that occurs wholly outside their borders,<sup>37</sup> the system as a whole is stable because states do not directly exercise law enforcement functions in other countries without first obtaining consent.<sup>38</sup>

In a similar vein, scholarship interrogating the extraterritorial aspects of law enforcement surveillance on the Internet has focused on the extraterritori-

- 
34. See, e.g., RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 432(2) (AM. LAW INST. 1987) ("A state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state, given by duly authorized officials of that state.").
  35. See, e.g., JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 156-58 (2006); Patricia L. Bellia, *Chasing Bits Across Borders*, 2001 U. CHI. LEGAL F. 35, 45-47; Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1205-13 (1998).
  36. See Goldsmith, *supra* note 35, at 1220-21 (arguing that the "threat of multiple regulation of cyberspace information flows" must be "measured by a regulation's enforceable scope," which is limited to persons and entities with presence or assets in the territory of the regulating state).
  37. As a matter of domestic law, Congress could in principle extend the reach of the criminal law as far as it likes, subject to constitutional limits. See John H. Knox, *A Presumption Against Extrajurisdictionality*, 104 AM. J. INT'L L. 351, 351 (2010). The Supreme Court has never clarified whether such limits exist. See *id.*; cf. Lea Brilmayer & Charles Norchi, *Federal Extraterritoriality and Fifth Amendment Due Process*, 105 HARV. L. REV. 1217, 1223 (1992) (arguing that constitutional due process "limits extraterritorial application of substantive federal law").
  38. See, e.g., RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 432(2); ROBERT CRYER ET AL., AN INTRODUCTION TO INTERNATIONAL CRIMINAL LAW AND PROCEDURE § 3.2.3, at 44 (2d ed. 2010) (defining "enforcement" (or "executive") jurisdiction as "the right to effect legal process coercively, such as to arrest someone, or undertake searches and seizures"); see also *Alvarez-Machain v. United States*, 331 F.3d 604, 625 (9th Cir. 2003) (en banc) ("Extraterritorial application [of a criminal statute], in other words, does not automatically give rise to extraterritorial enforcement authority."), *rev'd on other grounds sub nom. Sosa v. Alvarez-Machain*, 542 U.S. 692 (2004).

al scope of Fourth Amendment rights.<sup>39</sup> It lacks a thorough treatment of the interstate jurisdictional frictions that result and the implications such conduct might have on our conceptions of sovereignty, foreign relations, and Internet governance.

At the other end of the spectrum, the threat of harmful cross-border cyberoperations has become ever-present and raises questions about the capacity of states to protect their sovereign interests in territorial cyberinfrastructure.<sup>40</sup> There is a scholarly consensus that in theory, a cross-border cyberoperation could be characterized as an “internationally wrongful act” (permitting a state to respond with countermeasures under customary international law), a prohibited “use of force” (authorizing otherwise prohibited force in self-defense), or an “armed attack” (entitling harmed states to use otherwise prohibited force in self-defense), depending on the scope and severity of the damage caused by the operation.<sup>41</sup> States also use their domestic computer crime laws to criminalize cross-border cyberoperations by both state and nonstate actors that have effects in their territory.<sup>42</sup>

---

39. See, e.g., Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 380-87 (2015) (arguing that Fourth Amendment territoriality is a poor fit for regulating government collection of electronic data and discussing alternatives); Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285, 304-08 (2015) (arguing that virtual contacts alone are insufficient to create Fourth Amendment rights for foreign-located persons absent physical contacts or a legal relationship with the United States).

40. See Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1507 & n.19 (2013) (noting that “[v]irtually all legal scholarship approaches cyber-security from the standpoint of the criminal law or the law of armed conflict” and collecting the leading scholarship on both perspectives).

41. See, e.g., TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 36, 42-43, 45, 54 (Michael N. Schmitt ed., 2013) (presenting a nonbinding formulation of the international law norms applicable to cyberwarfare, unanimously agreed upon by a group of international experts brought together by the NATO Cooperative Cyber Defence Centre of Excellence); Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 839-57 (2012) (discussing the challenges of obtaining a consensus as to how an individual cyberattack *should* be classified despite the consensus that cyberattacks *could* be classified as a prohibited “internationally wrongful act,” “use of force,” or “armed attack”). For an extensive discussion of the debate surrounding the definition of “force” and “armed attack” in Articles 2(4) and 51 of the U.N. Charter, see Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT’L L. 421, 431-37 (2011).

42. In 2002, for example, Russian authorities charged an FBI agent with violating hacking and espionage laws by logging into a secure computer located in Russia and collecting data. See Mike Bruner, *FBI Agent Charged with Hacking*, NBC NEWS (Aug. 15, 2002), <http://www.nbcnews.com/id/3078784>. The FBI obtained log-on credentials from Russian hackers who were lured into the United States as part of an elaborate sting operation. *Id.* More recently, in 2014 U.S. authorities charged members of the Chinese military under U.S. economic espionage laws for exfiltration of intellectual property data from U.S. corporations. See Press Release, U.S. Dep’t of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor

*footnote continued on next page*

To be sure, the FBI's existing hacking techniques, properly executed, do not rise to the level of a cyber "armed attack," which would permit a state to respond with force under Article 51 of the U.N. Charter.<sup>43</sup> Nor is there an absolute prohibition on cross-border cyberoperations as a matter of international law.<sup>44</sup> But the scope of harm a cross-border cyberoperation might cause varies, as does interpretation of existing international norms.<sup>45</sup> Indeed, "[p]recisely when a non-consensual cyber operation violates the sovereignty of another State is a question . . . that ultimately will be resolved through the practice and opinio juris of States."<sup>46</sup> As such, the United States has an interest in leading the effort to clarify existing international norms as applied to government hacking and the development of norms through diplomatic measures.<sup>47</sup>

These circumstances highlight the failure of the existing rules to regulate the use of network investigative techniques. Rank-and-file law enforcement officials<sup>48</sup> have discretion over which crimes trigger the use of hacking techniques, the range of techniques that may be used once a warrant authorizes a search, and the ability to target computers of nonsuspects. Because the legal process governed by Rule 41 presumes that targets are territorially located, it does not consider the risk of potentially significant foreign relations consequences or encourage law enforcement to engage with foreign relations or national security experts in other parts of government.

This Article is the first to consider the cross-border implications of the use of network investigative techniques to pursue targets on the dark web and the institutional design problems that result. Broadly, it asks whether (and how) the legal architecture of cross-border investigations should adapt to the dark web, a space that defies our conceptions of geography and identity, and a reality where investigative activities for everyday crimes have a heightened

---

Organization for Commercial Advantage (May 19, 2014), <http://www.justice.gov/opa/pr/2014/May/14-ag-528.html>.

43. U.N. Charter art. 51. Forceful responses to hostilities below the threshold of an "armed attack" are only permissible with U.N. Security Council authorization. Specifically, Article 41 authorizes the Security Council to take measures that do not involve armed force, whereas Article 42 authorizes the Security Council to escalate measures to the use of armed force in the event nonforceful measures are inadequate. *See id.* arts. 41-42.
44. Brian J. Egan, Legal Advisor, U.S. Dep't of State, Remarks on International Law and Stability in Cyberspace, Address at Berkeley Law School (Nov. 10, 2016), <https://www.law.berkeley.edu/wp-content/uploads/2016/12/egan-talk-transcript-111016.pdf>.
45. *See infra* Part II.C.5.
46. Egan, *supra* note 44.
47. *Id.*
48. By "rank-and-file," this Article means "frontline agents who interface with the public." *See* John Rappaport, *Second-Order Regulation of Law Enforcement*, 103 CALIF. L. REV. 205, 210 (2015).

extraterritorial—and thus foreign relations—impact. More narrowly, it contends that extraterritorial aspects of network investigative techniques demonstrate the need for new substantive and procedural regulations that balance law enforcement goals with countervailing foreign relations interests.

This Article then identifies the failures of the existing legal process, suggests a number of substantive policy preferences that the executive branch should implement in response, and lays out a regulatory scheme for their implementation and enforcement that involves “a complex, dynamic interaction of institutions that simultaneously work together, challenge each other, defend themselves and divide responsibility.”<sup>49</sup> While the judiciary’s checks will remain essential to the implementation and enforcement of network investigative techniques, self-regulation within the executive branch and regulation from Congress are needed to produce decisions that are reliable, legitimate, and in the public interest.

This Article proceeds in three Parts. Part I describes how existing surveillance methods fail to solve crimes on the dark web and how the hacking techniques police use in response will unavoidably result in cross-border cyberexfiltration operations. Part II turns from the facts to the governing law, focusing on how the rules of criminal procedure limit the exercise of existing law enforcement functions to the territorial United States but fail to function in the same way when applied to network investigative techniques on the dark web. Cross-border cyberexfiltration operations are in obvious tension with international norms and thus raise a variety of foreign relations risks. Part III evaluates the shortcomings of the existing legal process and argues that a new regulatory framework is needed to govern network investigative techniques. It also offers initial thoughts as to what the new rules might look like and which institutions should set, implement, and enforce them.

Importantly, this Article does not attempt to resolve every issue prompted by the dark web or hacking techniques. Nor does it attempt to resolve the issue how states should regulate cross-border cyberoperations. Instead, it is intended to offer a policymaking framework for this new surveillance technology that minimizes immediate foreign relations and national security risks and allocates the authority to make new decisions on appropriate procedures to the institutions most competent to address them. To that end, the ultimate question is not how well the status quo functions but rather whether adjustments may produce better foreign relations outcomes without sacrificing law enforcement’s ability to identify and locate criminal suspects that have taken cover on the dark web.

---

49. See Edward L. Rubin, *Institutional Analysis and the New Legal Process*, 1995 WIS. L. REV. 463, 467 (book review).

## I. Law Enforcement in the Dark

### A. The Dark Web

The dark web is a private global computer network that enables users to conduct anonymous transactions without revealing any trace of their location. One such private network, whose characteristics I will use as a model for my analysis, is the Tor Network.<sup>50</sup> Computers on the Tor Network use an encrypted communications protocol that cannot be accessed using normal web browsers. Instead, they require the use of special software, like the Tor Browser. Proper use of the Tor Network makes it practically impossible for governments to trace the location of computers hosting “hidden” websites on the network, the location of computers accessing those hidden websites, or the location of computers that tunnel through the network to “anonymously” visit public websites on the World Wide Web.<sup>51</sup>

The Tor Network protects its users from two types of surveillance. First, it protects users from a common form of surveillance called “traffic analysis,” which is the real-time interception and examination of communications in order to deduce information.<sup>52</sup> Second, it prevents governments from using communications “metadata”—information *about* a communication, such as its source, destination, and size—acquired from third-party service providers to draw conclusions about the communicators and their behavior.<sup>53</sup>

---

50. The terms “dark web” and “Tor Network” are used interchangeably throughout this Article. The Tor Network was originally developed by the U.S. military and is now open source and publicly funded. See generally KRISTIN FINKLEA, CONG. RESEARCH SERV., R44101, DARK WEB 3 (2015); *Tor: Sponsors*, TOR PROJECT, <https://www.torproject.org/about/sponsors.html.en> (last visited Apr. 4, 2017) (listing past and present contributors to the Tor Network).

51. An “overlay network” is a computer network that is built on top of another network. Computers in the overlay network can be thought of as being connected by virtual or logical links, each of which corresponds to a path that often runs through many physical links, in the underlying physical network. Examples of overlay network deployments include virtual private networks, peer-to-peer networks such as Napster and BitTorrent, and Voice over Internet Protocol (VoIP) services such as Skype. See Guillermo Agustín Ibáñez Fernández, *New Computer Network Paradigms and Virtual Organizations*, in 2 GORAN D. PUTNIK & MARIA MANUELA CUNHA, ENCYCLOPEDIA OF NETWORKED AND VIRTUAL ORGANIZATIONS 1066, 1073 (2008); see also 2 IN LEE, HANDBOOK OF RESEARCH ON TELECOMMUNICATIONS PLANNING AND MANAGEMENT FOR BUSINESS 871 & tbl.2 (2009) (referring to overlay network deployments); Roger Dingledine et al., *Tor: The Second-Generation Onion Router* (n.d.), <https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf>.

52. See Stephen Northcutt, *Traffic Analysis*, SANS TECH. INST. (May 16, 2007), <http://www.sans.edu/cyber-research/security-laboratory/article/traffic-analysis>.

53. See Tony Gill, *Metadata and the Web*, in INTRODUCTION TO METADATA 20, 22 (Murtha Baca ed., 2d ed. 2008) (defining “metadata” as “a structured description of the essential attributes of an information object” (*italics omitted*)); David Talbot, *Dissent Made Safer*:  
*footnote continued on next page*

As a technical matter, the Tor Network protects users' communications from government surveillance because it disassociates communications "metadata" from communications "content" and bounces message packets off several intermediate computers, or "proxies," before steering them to their originally intended destination.<sup>54</sup> Proxy computers are scattered around the globe, provided by people who have volunteered their computers to the anonymity network.<sup>55</sup>

As a practical matter, the Tor Network can protect user communications from traffic analysis in two ways. First, users can "tunnel" through the Tor Network when communicating with publicly accessible webpages on the World Wide Web. As a result, when a user tunnels through the Tor Network in order to browse a webpage, her Internet traffic appears to originate at a proxy computer rather than at her true connection. Conversely, from the perspective of an ISP, traffic from the user's computer appears to be heading to another proxy computer rather than to the actual intended destination.

Thus, someone located in Seattle who has anonymized his communications using a series of proxies, the last of which is located in Italy, will appear to the destination webpage to be a user in Italy. Likewise, someone in Iran who has run his communications through a series of proxies, the last of which is located in San Francisco, will appear to the destination website as a web surfer from San Francisco and to the local ISP in Iran as though he were attempting to communicate with a proxy computer.

The second way people can use the Tor Network to protect their communications is through the Tor Network's hidden services feature, which allows people to host content or services without exposing the physical location of their servers. Hidden services are only accessible by those who use software

---

*How Anonymity Technology Could Save Free Speech on the Internet*, MIT TECH. REV. (Apr. 21, 2009), <https://www.technologyreview.com/s/413091/dissent-made-safer> ("In the United States, for example, libraries and employers often block content, and people's Web habits can be—and are—recorded for marketing purposes by Internet service providers (ISPs) and by the sites themselves.").

54. The Tor Network is currently maintained by the Tor Project, a 501(c)(3) nonprofit based in the United States and funded partly by a number of federal grants from the U.S. government. See Natascha Divac & Sam Schechner, *Munich Attack Investigation Shines Light on 'DarkWeb'*, WALL ST. J. (July 26, 2016, 9:03 PM ET), <https://www.wsj.com/articles/before-the-shootings-munich-gunman-visited-the-dark-web-1469558210>; Damian Paletta, *How the U.S. Fights Encryption—and Also Helps Develop It*, WALL ST. J. (Feb. 22, 2016, 12:31 AM ET), <http://www.wsj.com/articles/how-the-u-s-fights-encryptionand-also-helps-develop-it-1456109096>; see also *Tor: Sponsors*, *supra* note 50.
55. See FINKLEA, *supra* note 50, at 3-4, 4 n.20. As discussed in Part II.A below, foreign-located proxy computers are out of reach of U.S. subpoena authority unless their owners fall under the personal jurisdiction of U.S. courts (for instance, due to nationality or territorial presence).

that enables them to get on the Tor Network, and even then, communications between a hidden service (such as the Silk Road) and its users occur through a “rendezvous point,” a proxy that provides an additional layer of protection from traffic analysis.

Civil liberties advocates promote the use of the Tor Network to maintain free speech, privacy, and anonymity. For example, the Tor Network may be used to circumvent government censorship, enabling users to access online destinations that have been blocked by authoritarian regimes.<sup>56</sup> The Tor Network can also be used to facilitate spaces online where individuals can conduct sensitive communications without fear of being tracked. For example, individuals may want to anonymize their communications to research sensitive issues such as physical or mental illness or to engage in political dissent without government detection. Businesses may want to use the Tor Network to prevent corporate spies from gaining any competitive advantage by learning whom their employees are communicating with or what topics they are researching.

The added protection of the “hidden services” feature can also be used to circumvent a common censorship technique used by repressive regimes where websites deemed unfit for public consumption (such as blogs that promote dissent) are taken down and their web administrators arrested.<sup>57</sup> Journalists and whistleblower groups also use the Tor Network’s hidden services feature to communicate with sources. For example, SecureDrop, an open source whistleblower submission system initially created for the *New Yorker*, can be

---

56. Some governments have responded by enacting regulations around the use of the Tor Network or blocking access to known proxy nodes in the Tor Network. *See, e.g.,* Lorenzo Franceschi-Bicchierai, *Turkey Doubles Down on Censorship with Block on VPNs, Tor*, MOTHERBOARD (Nov. 4, 2016, 2:20 PM), <http://motherboard.vice.com/read/turkey-doubles-down-on-censorship-with-block-on-vpns-tor>. This, in turn, has led to the development of “bridge relay” technology that enables the user to gain access to the Tor Network by accessing Tor relays that are not listed in the main Tor directory (and thus are unknown to government censors). *See Tor: Bridges*, TOR PROJECT, <https://www.torproject.org/docs/bridges> (last visited Apr. 4, 2017).

57. If government agents are unable to locate the server hosting the blog, they cannot physically take it down (in the event it is located in-country) or request that a third party (or another country) do so. *See infra* Part I.B. Facebook set up a hidden services account in 2012. *See* Andy Greenberg, *Why Facebook Launched Its Own ‘Dark Web’ Site*, WIRED (Oct. 31, 2014, 12:31 PM), <https://www.wired.com/2014/10/facebook-tor-dark-site> (“[N]o surveillance system watching either Facebook’s connection or the user’s local traffic should be able to match up a user’s identity with their Facebook activity.”); Alec Muffett, *Making Connections to Facebook More Secure*, FACEBOOK (Oct. 31, 2014, 4:30 AM), <https://www.facebook.com/notes/protect-the-graph/making-connections-to-facebook-more-secure/1526085754298237>.

used by media organizations to securely accept documents from and communicate with anonymous sources.<sup>58</sup>

Not surprisingly, criminals and other malicious actors flocked to the dark web for its promise of an anonymous and secure platform for “conversation, coordination, and action.”<sup>59</sup> Modern criminals use the dark web to carry out technology-driven crimes, such as computer hacking, identity theft, credit card fraud, and intellectual property theft.<sup>60</sup> Platforms like the Silk Road provide a means for existing brick-and-mortar criminals to globalize their operations with virtual impunity. Increasingly, criminals use the dark web to facilitate crimes traditionally conducted in the physical world, such as currency counterfeiting,<sup>61</sup> drug distribution,<sup>62</sup> child exploitation,<sup>63</sup> human trafficking,<sup>64</sup> arms and ammunition sales,<sup>65</sup> assassination,<sup>66</sup> and terrorism.<sup>67</sup>

## B. Failure of Conventional Surveillance Methods

According to the DOJ, use of the dark web by criminals to anonymize communications makes it “impossible for law enforcement” to pursue criminal suspects.<sup>68</sup> In computer crime cases, locating the computer used by the perpetrator is the most critical step in discovering the perpetrator’s identity

---

58. Tom Lowenthal & Geoffrey King, *How SecureDrop Helps CPJ Protect Journalists*, COMMITTEE TO PROTECT JOURNALISTS (May 12, 2016, 7:00 AM), <https://cpj.org/x/686d>; see Lorenzo Franceschi-Bicchierai, *SecureDrop: Aaron Swartz’s Platform for Whistleblowers Rebooted*, MASHABLE (Oct. 15, 2013), <http://mashable.com/2013/10/15/secure-drop-aaron-swartz-freedom-of-the-press-foundation/#.Tu9ZMRgqkqm>.

59. See FINKLEA, *supra* note 50, at 8.

60. See *id.* at 8-10 (describing ways in which the dark web facilitates criminal activity).

61. Press Release, U.S. Dept of Justice, *Four Charged in International Uganda-Based Cyber Counterfeiting Scheme* (Apr. 2, 2015), <https://www.justice.gov/opa/pr/four-charged-international-uganda-based-cyber-counterfeiting-scheme>.

62. Press Release, U.S. Att’y’s Office for the S. Dist. of N.Y., *supra* note 1.

63. GOODMAN, *supra* note 1, at 206.

64. *Id.* at 207-08.

65. *Id.* at 205-06.

66. *Id.* at 206; see Andy Greenberg, *Meet the ‘Assassination Market’ Creator Who’s Crowdfunding Murder with Bitcoins*, FORBES (Nov. 18, 2013, 8:30 AM), <http://www.forbes.com/sites/andygreenberg/2013/11/18/meet-the-assassination-market-creator-whos-crowdfunding-murder-with-bitcoins/#2277df031ac1>.

67. According to German authorities, eighteen-year-old gunman Ali David Sonboly likely bought his handgun—which he used to kill nine people and himself in Munich on July 22, 2016—illegally on the dark web. Ruth Bender & Christopher Alessi, *Munich Shooter Likely Bought Reactivated Pistol on Dark Net*, WALL ST. J. (July 24, 2016, 4:23 PM ET), <http://www.wsj.com/articles/munich-shooter-bought-recommissioned-pistol-on-dark-net-1469366686>.

68. Letter from Mythili Raman to Judge Reena Raggi, *supra* note 25, at 2.

and collecting evidence to build a successful prosecution.<sup>69</sup> Without the perpetrator's laptop, investigators will lack evidence attributing virtual criminal conduct to an actual person.<sup>70</sup>

Conventional investigative methods rely on collection of data from third parties through compulsion and consent. When digital evidence is controlled by a person or entity subject to U.S. personal jurisdiction, compulsory process is used to obtain digital evidence. When digital evidence is outside U.S. jurisdiction—such as when it is controlled by an entity with no physical presence or assets in the United States—formal and informal law enforcement cooperation mechanisms are used to obtain it.

Investigators typically begin a computer crime investigation with nondescript information about the perpetrator's online alias, such as the e-mail address used to transmit communications.<sup>71</sup> Investigators may then decide to request all account information associated with the e-mail address from the third-party e-mail provider. In the event the e-mail service provider is beyond U.S. jurisdiction, the investigators will likely initiate protocols to use diplomatic channels to request that the host country provide the evidence. Before the advent of the dark web, the third-party disclosure would yield "true" identifying information—such as an Internet Protocol (IP) address registered with the ISP<sup>72</sup>—from which investigators could infer the user's log-on location.<sup>73</sup> Once the location of the device was determined, investigators could apply for a warrant to physically seize the device and extract its contents.<sup>74</sup>

---

69. Cf. Michael B. Mukasey, *The Attorney General's Guidelines for Domestic FBI Operations* 7 (2008), <http://www.usdoj.gov/ag/readingroom/guidelines.pdf> ("In most ordinary criminal investigations, the immediate objectives include . . . identifying, locating, and apprehending the perpetrators . . .").

70. See 3 PETER W. GREENWOOD ET AL., *NAT'L INST. OF JUSTICE, U.S. DEP'T OF JUSTICE, R-1778-DOJ, THE CRIMINAL INVESTIGATION PROCESS: OBSERVATIONS AND ANALYSIS* 65 (1975), <https://www.ncjrs.gov/pdffiles1/Digitization/148118NCJRS.pdf> (defining a "solved" case as one where investigators know "the identity of the perpetrator(s), even if additional work [is] needed to locate the perpetrators or to establish the facts needed to prove guilt in court").

71. See, e.g., *Sanders Affidavit*, *supra* note 17, ¶¶ 5-6, 11 (listing nondescript e-mail addresses used to communicate threatening messages to a school).

72. Cf. Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 284 (2005) ("In most cases, the biggest investigative lead comes in the form of an originating Internet Protocol (IP) address recorded by the bank's servers.")

73. Cf. Joshua J. McIntyre, Comment, *Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should Be Protected as Personally Identifiable Information*, 60 DEPAUL L. REV. 895, 912-13 (2011) (describing various technologies that enable IP geolocation).

74. See Kerr, *supra* note 72, at 285 ("The process of collecting electronic evidence in computer hacking cases generally divides into three steps. It begins with the collection of stored evidence from third-party servers, turns next to prospective surveillance, and ends with the forensic investigation of the suspect's computer.")

Increasingly, digital evidence is beyond U.S. jurisdiction. When evidence is *not* in the custody or control of a party that falls under U.S. jurisdiction, investigators use *consent-based* cross-border evidence collection methods, implemented through a series of formal and informal relationships.<sup>75</sup> The principal and least controversial tool for evidence collection in such cases is a Mutual Legal Assistance Treaty (MLAT).<sup>76</sup> MLATs facilitate law enforcement cooperation and assistance in support of ongoing criminal investigations or proceedings.<sup>77</sup> MLATs generally contain provisions for locating and identifying persons and items, serving process, executing search warrants, taking witness depositions, summoning witnesses; and seizing assets.<sup>78</sup>

MLATs are negotiated by the U.S. Department of State<sup>79</sup> and implemented by the DOJ's Office of International Affairs (OIA), the DOJ's foreign relations office.<sup>80</sup> Once the agreement goes into force, the OIA is the "[c]entral [a]uthority" tasked with working with "foreign counterparts to ensure effective treaty implementation."<sup>81</sup> The OIA also serves an interdepartment coordination role, briefing "the Attorney General and other senior [DOJ] officials on international issues and provid[ing] advice on sensitive law enforcement matters that could impact the foreign relations and strategic interests of the United States."<sup>82</sup>

In addition to formal diplomatic mechanisms, federal law enforcement actors exchange criminal investigation-related information through informal channels and relationships cultivated to facilitate interstate law enforcement cooperation and access to evidence.<sup>83</sup> The United States also engages in joint investigations, which are coordinated investigative efforts among law enforcement agencies of different countries in criminal matters.<sup>84</sup>

---

75. In the past, the use of network investigative techniques overseas has relied on consent-based mechanisms. *See infra* note 115 and accompanying text.

76. *See* 7 U.S. DEP'T OF STATE, FOREIGN AFFAIRS MANUAL § 962.1 (2013) (providing a brief historical overview of MLATs and a list of bilateral MLATs in force).

77. *See id.* § 962.1(a).

78. *See id.*

79. *See id.* § 962.1.

80. *See Frequently Asked Questions Regarding Evidence Located Abroad*, U.S. DEP'T JUST., <http://www.justice.gov/criminal-oia/frequently-asked-questions-regarding-evidence-located-abroad> (last updated June 11, 2015).

81. *Office of International Affairs (OIA)*, U.S. DEP'T JUST., <https://www.justice.gov/criminal-oia> (last visited Apr. 4, 2017).

82. *Id.*

83. *See Frequently Asked Questions Regarding Evidence Located Abroad*, *supra* note 80.

84. *See, e.g.*, *United States v. Emmanuel*, 565 F.3d 1324, 1328, 1330 (11th Cir. 2009); *In re Terrorist Bombings of U.S. Embassies in E. Afr.*, 552 F.3d 157, 159-60 (2d Cir. 2008); *United States v. Barona*, 56 F.3d 1087, 1089-93 (9th Cir. 1995); *United States v. Behety*, 32 F.3d 503, 510-11 (11th Cir. 1994); *United States v. Marzook*, 435 F. Supp. 2d 708, 775-

*footnote continued on next page*

Consider an elementary school that receives a series of bomb threats by e-mail.<sup>85</sup> The perpetrator uses a nondescript e-mail address and leaves no clues that can be used to discover his true identity.<sup>86</sup> Instead, investigators must follow the digital trail the perpetrator's computer has laid out. Investigators will likely first subpoena the e-mail service provider whose services were used to communicate the threat, requesting disclosure of evidence associated with the perpetrator's account.<sup>87</sup> If the ISP does not fall under U.S. jurisdiction—for example, if it is located in Italy—investigators will use formal and informal mechanisms to seek assistance from cooperating agencies abroad. Investigators may pursue formal procedures, calling the OIA and triggering the MLAT protocols in Italy. The lead investigator may also use informal channels, such as his personal relationships with foreign law enforcement authorities. Either way, the ISP's disclosure will likely include an IP "address log" detailing the activity history for the e-mail address.<sup>88</sup>

Use of the dark web by the perpetrator, however, renders these conventional evidence collection methods obsolete. Recall that when someone tunnels through the dark web to browse a public webpage, his Internet traffic appears to originate from one of thousands of "proxy" computers rather than the one he is using.<sup>89</sup> Without the ability to obtain a true location for the targeted device, investigators are unable to initiate conventional evidence collection protocols.

---

77 (N.D. Ill. 2006); *United States v. Castro*, 175 F. Supp. 2d 129, 132-33 (D.P.R. 2001); cf. ORGANISATION FOR ECON. CO-OPERATION & DEV., *TYPOLGY ON MUTUAL LEGAL ASSISTANCE IN FOREIGN BRIBERY CASES* 51 (2012), <http://www.oecd.org/daf/anti-bribery/TypologyMLA2012.pdf> (describing "Joint Investigative Teams," which are used by European Union member countries and allow "two or more countries to form a team to conduct a single criminal investigation").

85. This hypothetical is loosely based on a case from 2007. See *Sanders Affidavit*, *supra* note 17, ¶ 11.

86. Cf. *id.* ¶ 6.

87. See 18 U.S.C. § 2703(c)(2) (2015) (requiring third-party ISPs to disclose user account information with a subpoena).

88. If the ISP keeps comprehensive records, additional information such as a billing address may also be disclosed. *Id.*; see *Kerr*, *supra* note 72, at 286 n.11 (citing *United States v. Kennedy*, 81 F. Supp. 2d 1103, 1107 (D. Kan. 2000), as an example of a case where the customer's billing address and telephone number were disclosed). Once a suspect is identified, investigators and prosecutors decide whether there is sufficient evidence to bring a successful prosecution. See *Kerr*, *supra* note 72, at 289. The suspect's true identity opens up the door to all sorts of evidence and investigation methods. This may include indirect collection of digital evidence (for instance, in the form of e-mails, GPS, and telephony data) from third parties through compelled disclosure. See 18 U.S.C. §§ 2701-2711; see also *infra* Part II.A. This may also include direct collection, authorized by warrant, in the form of physical surveillance methods or collection of digital evidence from the device used to perpetrate the crime. See *infra* Part II.B.

89. See *supra* Part I.A.

In the dark web version of our hypothetical, the suspect tunnels through the dark web to anonymize a connection to a third-party e-mail service provider. Thus, surveillance methods that depend on disclosures from third-party ISPs can no longer be used to locate investigation targets.<sup>90</sup> Investigators are still authorized to subpoena the e-mail provider for relevant account information. However, this time, the third-party disclosures reveal to investigators *only* that the suspect anonymized his communications.<sup>91</sup> The investigators are unable to physically seize the computer, whether through direct means or with the cooperation of another country. With no other leads, the investigation grinds to a halt.<sup>92</sup>

Use of the dark web by criminal actors enables secret, untraceable criminal activity to take place at scale.<sup>93</sup> The existence of hidden services like the Silk Road “dramatically lower[s] the entry barriers into the underground

---

90. See Kerr, *supra* note 72, at 286.

91. The investigators know this because the IP address received is that of a known “proxy” computer. When someone using the Tor Network browses a webpage, his Internet traffic appears to originate from one of hundreds of Tor’s exit nodes rather than his home connection, and the communication cannot be traced backwards. Conversely, from the perspective of an ISP on the originating end, traffic from the Tor user appears to be heading toward one of hundreds of Tor’s entry nodes rather than the actual intended destination. As a result, law enforcement can no longer use third-party disclosures to identify a target. See generally FINKLEA, *supra* note 50, at 3-5.

92. Notably, in all publicly available warrant applications reviewed by the Author, the application affiant has asserted that locating the true IP address of the perpetrator is impossible but for the use of network investigative techniques. For example, one affidavit stated:

Due to the unique nature of the Tor network and the method by which the network protects the anonymity of its users by routing communications through multiple other computers or “nodes,” . . . other investigative procedures that are usually employed in criminal investigations of this type have been tried and have failed or reasonably appear to be unlikely to succeed if they are tried.

Affidavit of Special Agent Douglas Macfarlane in Support of Application for Search Warrant ¶ 31, *In re Search of Computs. That Access upf45jv3bziuctml.onion*, No. 1:15-SW-89 (E.D. Va. Feb. 20, 2015); see also *United States v. Arterbury*, No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67091, at \*5-6 (N.D. Okla. Apr. 25, 2016) (“The critical point is that without the use of such techniques as [network investigative techniques], agents seeking to track a Tor user to his home computer will not be able to take that pursuit beyond the exit node from which the Tor user accessed the regular Internet.”), *report and recommendation adopted by* 2016 U.S. Dist. LEXIS 67092 (N.D. Okla. May 17, 2016).

93. It is perhaps for this reason that the FBI considers computer crimes to be “the most significant crimes confronting the United States.” FINKLEA, *supra* note 50, at 9; see also James B. Comey, Dir., FBI, *The FBI and the Private Sector: Closing the Gap in Cyber Security*, Remarks at the RSA Cyber Security Conference (Feb. 26, 2014), <https://www.fbi.gov/news/speeches/the-fbi-and-the-private-sector-closing-the-gap-in-cyber-security> (“Before he left, Director Mueller told me that he believed cyber issues would come to dominate my tenure as counterterrorism had dominated his time as Director. And I believe he is right. We must be agile and predictive on every front. And we must use every tool and authority at our disposal to stop these malicious activities.”).

economy—for both buyers and sellers alike.”<sup>94</sup> The resurgence of several underground marketplaces in the wake of the Silk Road shutdown underscores the asymmetry between investigators’ ability to track unlawful activity and criminals’ capacity to commit crimes on the dark web.<sup>95</sup>

### C. Hacking as an Investigative Tool on the Dark Web

Anonymity tools are not the first technological change to leapfrog law enforcement surveillance capabilities.<sup>96</sup> The FBI has termed this leapfrog phenomenon “going dark.”<sup>97</sup> In the 1990s, for instance, law enforcement lost its ability to wiretap calls when telephone companies switched from copper cables to digital telephony.<sup>98</sup> The result was the passage of the Communications Assistance for Law Enforcement Act in 1994, which required telephone carriers to install standardized equipment so they could assist police with electronic wiretaps.<sup>99</sup> However, such “backdoor” solutions are not technologically feasible on the dark web due to its decentralized architecture, use of open software, and core functionality requirements.<sup>100</sup>

Network investigative techniques circumvent the challenges the dark web poses by using the Internet to facilitate the delivery and installation of surveillance software (malware<sup>101</sup>) on the target device.<sup>102</sup> Formerly, an

---

94. Government Sentencing Submission, *supra* note 15, at 2.

95. *See id.* at 3, 13; Press Release, Sen. Tom Carper, *supra* note 14.

96. Bellovin et al., *supra* note 18, at 8-18 (providing a history of communications technologies leapfrogging law enforcement capabilities, including cellular telephony, VoIP, and end-to-end encryption). *See generally* William J. Stuntz, *Race, Class, and Drugs*, 98 COLUM. L. REV. 1795, 1804 (1998) (noting that criminals generally have an incentive to change patterns once law enforcement agencies adapt).

97. *Going Dark*, FED. BUREAU INVESTIGATION, <https://www.fbi.gov/services/operational-technology/going-dark> (last visited Apr. 4, 2017) (describing the “going dark” issue as the FBI’s inability to access evidence due to technological barriers).

98. Bellovin et al., *supra* note 18, at 7 (noting that with the advent of digital telephony it was no longer possible to tap lines with the traditional method of “two alligator clips and a tape recorder”).

99. *See id.* at 6-7; *see also* Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, § 103, 108 Stat. 4279, 4280-82 (1994) (codified as amended at 47 U.S.C. § 1002 (2015)).

100. Bellovin et al., *supra* note 18, at 6-7, 18. A thorough discussion of how the open, distributed architecture of certain anonymity tools makes technological backdoors infeasible is beyond the scope of this Article. For our purposes, it is sufficient to know that (1) distributing a technology’s network architecture may place its components beyond a state’s jurisdictional reach and (2) using open architecture allows transferability of components by independent third parties.

101. *See supra* note 17.

102. *See* Memorandum from Sara Sun Beale & Nancy King to Advisory Comm. on Rules of Criminal Procedure, *supra* note 32, at 2 (describing network investigative techniques as  
*footnote continued on next page*

investigator wishing to search a computer using conventional methods had to gain access to the physical location of the computer and generate a copy of its hard drive. This requires knowledge of the computer's physical location, which the dark web obscures.

Network investigative techniques create a way for investigators to reach a computer that does not require knowledge of its physical location. Rather than traversing "physical" pathways—such as roads and bridges—to reach the target's physical address, investigators deploy malware that traverses "virtual" pathways—such as connections between computers and bridges between networks—to reach the computer's virtual IP address. Importantly, the new methods can reach the same destination.<sup>103</sup> Once malware penetrates the target, it converts the computer into a surveillance device.

Network investigative techniques function in two steps: access to data and extraction of data.<sup>104</sup> The "access" step can be thought of as arriving at the location of a file cabinet and picking its lock,<sup>105</sup> and the "extraction" step can be thought of as rifling through the file cabinet's contents.<sup>106</sup>

---

"remote access searches, in which the government seeks to obtain access to electronic information or an electronic storage device by sending surveillance software over the Internet").

103. A physical search requires knowing the *physical* location of a target computer. By contrast, a remote search requires a means to communicate with the target computer, such as an active e-mail address. *See infra* notes 107-12 and accompanying text.
104. Description and analysis of predeployment and postexecution steps are beyond the scope of this Article. Of course, there are important steps that occur before deployment, such as vulnerability harvesting (analogized to gaining knowledge about the various types of locks that are in use by file cabinet makers and how to unlock them) and target reconnaissance (analogized to figuring out what types of locks a particular target uses and whether the attacker can access them). *See generally* Bellovin et al., *supra* note 18, at 34-41.
105. The "access" step requires two critical pieces of information: (1) the existence of a software vulnerability and (2) an available path or "attack vector" to successfully access and exploit that vulnerability. *Cf.* NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 83 (William A. Owens et al. eds., 2009) [hereinafter NRC REPORT] ("Access would be an available path for reaching the file cabinet . . ."). A vulnerability can be analogized to a faulty lock on the file cabinet. It is a security flaw or weakness that can be used by an attacker to compromise the system. A vulnerability can be (1) a code-based vulnerability, such as a weakness in the browser application used by the target; (2) a human vulnerability, where the weakness is a human who possesses credentials needed to access a system; or (3) a combination of the two, where a human vulnerability enables the attacker to deceive the user into performing an act that would (indirectly) cause the system to be compromised. At any rate, the relevant state action for the "access" step of our analysis is the execution of the attack vector to access and exploit a particular software or hardware vulnerability.
106. *Id.* ("The payload is the action taken by the intruder after the lock is picked.").

In the access step, law enforcement deploys malware that travels across the Internet to the target device, where it exploits a software security vulnerability that enables access to the system.<sup>107</sup> As in the physical world, an investigator may take one of many different paths in cyberspace to reach the location of a target. To that end, deployment mechanisms divide into three categories: spear phishing attacks, watering hole operations, and man-in-the-middle attacks. In a “spear phishing” operation, law enforcement targets an individual device by sending the target a communication (typically through e-mail or social media) to convince her to take a particular action—such as clicking on a link or opening an attachment—that triggers the delivery of malware.<sup>108</sup> In a “watering hole” operation, investigators first gain control of a server and then use it to distribute attacks to all visitors.<sup>109</sup> And in a “man-in-the-middle” attack, investigators lodge themselves between two endpoints of a communication so they can secretly relay or alter communications between parties.<sup>110</sup>

In the extraction step, a set of malware instructions known as a “payload” is executed on the device, effectively turning it into a surveillance tool.<sup>111</sup> Once installed, malware can cause a computer to perform any task the computer is capable of performing. For example, it may direct files and communications to a server controlled by law enforcement or gather images and sound at any time

---

107. See *id.* at 86-87; Bellovin et al., *supra* note 18, at 25-26.

108. See Jennifer Valentino-DeVries & Danny Yadron, *FBI Taps Hacker Tactics to Spy on Suspects*, WALL ST. J. (Aug. 3, 2013, 3:17 PM ET), <http://on.wsj.com/14mj2pV> (noting that investigators “us[e] a document or link that loads software when the [targeted] person clicks or views it”); cf. Tom N. Jagatic et al., *Social Phishing*, COMM. ACM, Oct. 2007, at 94, 94, 96 (demonstrating empirically that phishing attacks impersonating a friend of the target are more successful than those in which the sender is not known to the target).

109. See, e.g., Darien Kindlund, *Holiday Watering Hole Attack Proves Difficult to Detect and Defend Against*, ISSA J., Feb. 2013, at 10, 11 (describing a watering hole attack that infected visitors of a certain page on the website of the Council of Foreign Relations); Ellen Nakashima, *This Is How the Government Is Catching People Who Use Child Porn Sites*, WASH. POST (Jan. 21, 2016), <http://wpo.st/nom72> (describing the use of watering hole attacks used to hack computers that visit hidden child pornography sites).

110. Bellovin and his coauthors describe a man-in-the-middle attack as follows:

A Man-in-the-Middle attack is a method of gaining access to target information in which an active attacker interrupts the connection between the target and another resource and surreptitiously inserts itself as an intermediary. This is typically done between a target and a trusted resource, such as a bank or email server. To the target the attacker pretends to be the bank, while to the bank the attacker pretends to be the target. Any authentication credentials required (e.g., passwords or certificates) are spoofed by the attacker, so that each side believes they are communicating with the other. But because all communications are being transmitted through the attacker, the attacker is able to read and modify any messages it wishes to.

Bellovin et al., *supra* note 18, at 24 (bolding omitted).

111. See NRC REPORT, *supra* note 105, at 88.

the executing agent chooses.<sup>112</sup> From behind a screen at the other end of the connection, investigators are able to deploy immensely powerful techniques that scale with ease to track and surveil suspects.

But consider this important wrinkle: the clear majority of dark web users are *outside* the territorial United States.<sup>113</sup> And because each computer's location is theoretically indistinguishable from the next, any law enforcement target pursued on the dark web may be located overseas.<sup>114</sup>

The overseas cyberexfiltration operations that result from the use of network investigative techniques are a significant change in the way U.S. law enforcement engages in cross-border investigations. Before the amendment to Rule 41, criminal legal process authorized methods for evidence collection that aligned with customary international law, where it is considered an incursion on another state's sovereignty to carry out law enforcement functions within another state without that state's consent. To that end, law enforcement agencies relied on the United States' diplomatic relations and treaties with other countries, seeking permission from the host state before deploying personnel and requesting assistance from local authorities to collect foreign-located evidence when possible. For instance, the Drug Enforcement Administration has recently confirmed that it has used hacking tools on seventeen devices in a foreign country pursuant to a foreign court order and with the cooperation of foreign officials.<sup>115</sup>

In contrast to conventional methods, the exercise of extraterritorial law enforcement functions will be unilateral. It will not be limited to matters of national security, nor will it be coordinated with the State Department or other relevant agencies.<sup>116</sup> Case-by-case investigatory decisions made by rank-and-file officials<sup>117</sup> will have direct overseas consequences. The foreign

---

112. See *In re Warrant to Search a Target Comput. at Premises Unknown*, 958 F. Supp. 2d 753, 755-56, 761 (S.D. Tex. 2013) (denying on territorial limitation grounds an application for a warrant to use network investigative techniques that control the computer's camera and calculate the latitude and longitude of the device); see also Timberg & Nakashima, *supra* note 18 (describing features of network investigative techniques).

113. See *Top-10 Countries by Relay Users*, *supra* note 28 (estimating that around 20% of the Tor Network's daily users are based in the United States).

114. Targeting on the dark web is blind; investigators do not know where the target is located and thus cannot control the route network investigative techniques take to get there. See Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1072-73 (2001).

115. See Letter from Peter J. Kadzik, Assistant Att'y Gen., U.S. Dep't of Justice, to Sen. Charles E. Grassley, Chairman, Senate Judiciary Comm. 2 (July 14, 2015) (on file with author).

116. Ghappour, *supra* note 26.

117. See *supra* note 48.

relations risks that may be incurred call into question the wisdom of allowing rank-and-file officials to drive decisionmaking as to what crimes should trigger the use of hacking techniques, what hacking techniques should be used, and whose property interests may be targeted.

## II. Law Enforcement out of Bounds

### A. Conventional Methods Are in Harmony with International Law

International law delimits one state's power over another state's territorial sovereignty<sup>118</sup> by restricting states' exercise of prescriptive, adjudicative, and enforcement jurisdiction.<sup>119</sup> In the context of criminal law, the United States exercises *prescriptive* jurisdiction when Congress enacts statutes that criminalize conduct and *enforcement* jurisdiction when its law enforcement agencies investigate, apprehend, or prosecute a wrongdoer.<sup>120</sup>

Prescriptive jurisdiction and enforcement jurisdiction "are not geographically coextensive."<sup>121</sup> International law is most permissive with respect to

---

118. Territorial sovereignty can be defined as the principle that each state is coequal and has the final authority within its territorial limits. See Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 IND. J. GLOBAL LEGAL STUD. 475, 476 & n.5 (1998) (citing Stephen D. Krasner, *Sovereignty: An Institutional Perspective*, 21 COMP. POL. STUD. 66, 86 (1988) ("The assertion of final authority within a given territory is the core element in any definition of sovereignty."); and Janice E. Thomson, *Sovereignty in Historical Perspective: The Evolution of State Control over Extraterritorial Violence*, in THE ELUSIVE STATE: INTERNATIONAL AND COMPARATIVE PERSPECTIVES 227, 227 (James A. Caporaso ed., 1989) ("Despite their debate over whether the state is a withering colossus or a highly adaptive entity . . . , international relations theorists agree on an even more fundamental point. Both liberal interdependence and realist theories rest on the assumption that the state controls at least the principal means of coercion."); see also *Island of Palmas (U.S. v. Neth.)*, 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928) ("Sovereignty in the relations between States signifies . . . the right to exercise [on its territory], to the exclusion of any other States, the functions of a State.").

119. Broadly, "jurisdiction" can be defined as a state's "right under international law to regulate matters not exclusively of domestic concern." See F.A. Mann, *The Doctrine of Jurisdiction in International Law*, 111 RECUEIL DES COURS 9, 9 (1964). "Prescriptive jurisdiction" refers to a state's ability "to make its law applicable to the activities, relations, or status of persons, or the interests of persons in things." RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 401(a) (AM. LAW INST. 1987). "Adjudicative jurisdiction" is defined as a state's ability "to subject persons or things to the process of its courts or administrative tribunals." *Id.* § 401(b). "Enforcement jurisdiction" refers to a state's ability to "compel compliance . . . with its laws." *Id.* § 401(c).

120. See RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 432(1).

121. *FTC v. Compagnie de Saint-Gobain-Pont-a-Mousson*, 636 F.2d 1300, 1316 (D.C. Cir. 1980).

prescriptive jurisdiction. It permits a state to criminalize conduct that occurs beyond its borders so long as the prescribed conduct has territorial effects.<sup>122</sup> But “[a] state having jurisdiction to prescribe a rule of law does not necessarily have jurisdiction to enforce it in all cases.”<sup>123</sup> “[U]nlike a state’s prescriptive jurisdiction, which is not strictly limited by territorial boundaries, enforcement jurisdiction by and large continues to be strictly territorial.”<sup>124</sup> Indeed, there is unanimous consensus among states that “no state may engage in an act of coercion in the territory of another state without the latter’s consent.”<sup>125</sup>

Thus, while Congress may criminalize conduct that occurs wholly overseas so long as it has domestic “effects,”<sup>126</sup> international law forbids U.S. investigators from directly exercising law enforcement functions in other countries without first obtaining consent.<sup>127</sup> “[A] state cannot investigate a

- 
122. See *United States v. Aluminum Co. of Am.*, 148 F.2d 416, 443 (2d Cir. 1945) (“[A]ny state may impose liabilities, even upon persons not within its allegiance, for conduct outside its borders that has consequences within its borders which the state reprehends . . .”). The application of federal statutes to overseas acts is permissible under international law only if the criminalized conduct has or is intended to have harmful effects on U.S. territory, nationals, or security interests; is a universally condemned offense; or was committed by a U.S. national. See *Draft Convention on Jurisdiction with Respect to Crime*, 29 AM. J. INT’L L. 435, 439-42 (Supp. 1935); see also INT’L BAR ASS’N, REPORT OF THE TASK FORCE ON EXTRATERRITORIAL JURISDICTION 11-16 (2009), <http://www.ibanet.org/Document/Default.aspx?DocumentUid=ECF39839-A217-4B3D-8106-DAB716B34F1E> (noting that “states have long recognized the right of a state to exercise jurisdiction over persons or events located outside its territory in certain circumstances, based on the effects doctrine, the nationality or personality principle, the protective principle[,] or the universality principle” and providing an overview of each basis of jurisdiction).
123. *Saint-Gobain*, 636 F.2d at 1316 (alteration in original) (quoting RESTATEMENT (SECOND) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 7(1) (AM. LAW INST. 1965)).
124. *Id.*; see also Hannah L. Buxbaum, *Territory, Territoriality, and the Resolution of Jurisdictional Conflict*, 57 AM. J. COMP. L. 631, 664 (2009).
125. Buxbaum, *supra* note 124, at 664; see also RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 432(2); JAMES CRAWFORD, BROWNLIE’S PRINCIPLES OF PUBLIC INTERNATIONAL LAW 478-79 (8th ed. 2012). The principle of nonintervention prohibits all acts that are intended “to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind.” G.A. Res. 2625 (XXV), annex, Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations (Oct. 24, 1970).
126. As a matter of domestic law, Congress may extend the reach of the criminal law extraterritorially, subject to constitutional limits. Knox, *supra* note 37, at 351 n.1 (“Congress could decide to exceed [international law limits] if it chose to place the United States in violation of international law.”); see Brilmayer & Norchi, *supra* note 37, at 1223 (arguing for jurisdictional limits on legislative authority that sound in constitutional due process).
127. See, e.g., RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 432(2) (“A state’s law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state, given by duly
- footnote continued on next page*

crime, arrest a suspect, or enforce its judgment or judicial processes in another state's territory without the latter state's permission."<sup>128</sup> Nonetheless, using conventional mechanisms, U.S. criminal investigators collect digital evidence located anywhere in the world while limiting the exercise of enforcement mechanisms to the territorial United States.<sup>129</sup>

The evidence collection methods authorized under the pre-amendment version of the Federal Rules of Criminal Procedure are in harmony with international law's restrictions on enforcement jurisdiction. Despite their global reach, the rules of criminal procedure may only be enforced with respect to persons and property that touch the United States.<sup>130</sup>

In this context, digital evidence collection can be divided into direct and indirect collection mechanisms. Direct collection typically involves coerced entry<sup>131</sup> into a place by government actors for the purpose of acquiring evidence of a crime, and it typically requires a search warrant.<sup>132</sup> Indirect collection, by contrast, involves service of a subpoena or court order that

---

authorized officials of that state."); *CRYER ET AL.*, *supra* note 38, § 3.2.3, at 44 (using the term "executive jurisdiction" to discuss enforcement jurisdiction and defining it as "the right to effect legal process coercively, such as to arrest someone, or undertake searches and seizures"); *see also Alvarez-Machain v. United States*, 331 F.3d 604, 625 (9th Cir. 2003) (en banc) ("Extraterritorial application [of a criminal statute] . . . does not automatically give rise to extraterritorial enforcement authority."), *rev'd on other grounds sub nom. Sosa v. Alvarez-Machain*, 542 U.S. 692 (2004).

128. INT'L BAR ASS'N, *supra* note 122, at 10.

129. *See infra* notes 130-53 and accompanying text.

130. Cf. 1 OPPENHEIM'S INTERNATIONAL LAW: PEACE 432 (Robert Jennings & Arthur Watts eds., 9th ed. 1992) ("[T]he interference must be forcible or dictatorial, or otherwise coercive, in effect depriving the state intervened against of control over the matter in question."); Maziar Jamnejad & Michael Wood, *The Principle of Non-Intervention*, 22 LEIDEN J. INT'L L. 345, 372 (2009) ("The exercise of enforcement jurisdiction in the territory of another state, without its consent, breaches the non-intervention principle. . . . [E]xtraterritorial enforcement measures will nearly always be considered illegal [under customary international law].").

131. Direct collection includes forcibly entering a space where the targeted device is located and subsequently bypassing security restrictions on that device. However, entry or access need not cause physical damage to be "coerced." *See, e.g., Calabretta v. Floyd*, 189 F.3d 808, 813 (9th Cir. 1999).

132. This type of government conduct typically falls under the Warrant Clause of the Fourth Amendment, which requires investigators to first obtain a search warrant before performing the collection activity. *See* U.S. CONST. amend. IV. A search warrant constitutes the judicial authorization, made upon a finding of probable cause, of an activity that is uniquely assigned to law enforcement—intruding upon an individual's reasonable expectation of privacy to conduct a search and seizure. A search warrant is self-executing; it authorizes an investigator to directly coerce entry or access to, and extraction of digital evidence from, a computer or electronic media. *See, e.g., Marshall v. Barlow's, Inc.*, 436 U.S. 307, 316 (1978) (explaining that searches may be "executed without delay and without prior notice, thereby preserving the element of surprise"); *see also Search Warrant*, BLACK'S LAW DICTIONARY (10th ed. 2014).

imposes an affirmative duty on its recipient to either produce evidence under that recipient's control or face sanctions for noncompliance.<sup>133</sup> In the digital context, a physical seizure of a computer is a direct collection, as is the use of network investigative techniques. The subpoena power, on the other hand, is an indirect collection mechanism, as is the use of compelled technical assistance to conduct a wiretap.

Direct collection of foreign-located evidence using conventional methods is an obvious exercise of enforcement jurisdiction.<sup>134</sup> Criminal procedure requires direct collection of digital evidence to be conducted pursuant to a search warrant, which authorizes investigators to exercise coercive "search and seizure" powers directed toward a particular place to be searched or thing to be seized.<sup>135</sup> Investigators executing a search warrant may use coercive force and may even damage the targeted items or premises when necessary to effectuate a particular search or seizure.<sup>136</sup>

Search warrant authority (and direct collection methods exercised under search warrant authority) does not generally extend beyond the territorial United States.<sup>137</sup> Federal Rule of Criminal Procedure 41 generally restricts a

---

133. See, e.g., *In re Grand Jury Proceedings the Bank of N.S.*, 740 F.2d 817, 829 (11th Cir. 1984) (holding that a Canadian bank operating in the United States was obliged to produce documents located in the Cayman Islands in response to a grand jury subpoena); see also *In re Grand Jury Subpoena Directed to Marc Rich & Co.*, 707 F.2d 663, 667 (2d Cir. 1983) ("The test for the production of documents is control, not location.").

134. As Justice Joseph Story explained in 1841, territorial sovereignty implies that "no state or nation can, by its laws, directly affect, or bind property out of its own territory, or bind persons not resident therein." JOSEPH STORY, COMMENTARIES ON THE CONFLICT OF LAWS, FOREIGN AND DOMESTIC, IN REGARD TO CONTRACTS, RIGHTS, AND REMEDIES, AND ESPECIALLY IN REGARD TO MARRIAGES, DIVORCES, WILLS, SUCCESSIONS, AND JUDGMENTS § 20 (Boston, Charles C. Little & James Brown 2d ed. 1841) (emphasis added); see also Goldsmith, *supra* note 118, at 480.

135. See, e.g., *Riley v. California*, 134 S. Ct. 2473, 2485 (2014) (holding that officers must generally secure a search warrant before conducting a search of data stored on a smartphone confiscated incident to a lawful arrest); *Calabretta*, 189 F.3d at 813 ("The principle that government officials cannot coerce entry into people's houses without a search warrant or applicability of an established exception to the requirement of a search warrant is so well established that any reasonable officer would know it.").

136. See, e.g., *In re Subpoena Duces Tecum*, 228 F.3d 341, 348 (4th Cir. 2000) ("To preserve advantages of speed and surprise, [a warrant] is issued without prior notice and is executed, often by force, with an unannounced and unanticipated physical intrusion.").

137. In 1990, the Supreme Court, ruling that foreign-located nonresident aliens are not entitled to Fourth Amendment protection, strongly suggested that the Warrant Clause has no extraterritorial application. *United States v. Verdugo-Urquidez*, 494 U.S. 259, 274-75 (1990); see also *In re Terrorist Bombings of U.S. Embassies in E. Afr.*, 552 F.3d 157, 169 (2d Cir. 2008) ("[I]n *Verdugo-Urquidez*, seven justices of the Supreme Court endorsed the view that U.S. courts are not empowered to issue warrants for foreign searches."); *United States v. Barona*, 56 F.3d 1087, 1092 n.1 (9th Cir. 1995) ("[F]oreign searches have neither been historically subject to the warrant procedure, nor could they be as a practical matter."); *United States v. Bin Laden*, 126 F. Supp. 2d 264, 275 (S.D.N.Y. 2000)

*footnote continued on next page*

court's authority to issue warrants to the district of the magistrate making the decision.<sup>138</sup> Exceptions are generally limited to instances in which the search warrant relates to American diplomatic or consular missions in foreign states.<sup>139</sup> Indeed, any collection of evidence that requires an assertion of extraterritorial enforcement jurisdiction triggers the formal and informal cooperation protocols discussed in Part I.B above.

Indirect collection of foreign-located evidence, by contrast, does not require the exercise of enforcement jurisdiction overseas. Instead, compelled disclosure orders impose an affirmative duty on third parties to disclose evidence in their possession or control in response to a specific request.<sup>140</sup> A person or entity that fails to produce evidence in its control may face domestic sanctions for noncompliance.<sup>141</sup> Critically, the steps of the collection act—accessing and extracting foreign-located data—are performed by third parties, not state actors.<sup>142</sup>

In practice, courts regularly issue and uphold orders that compel disclosure of foreign-located evidence from third parties, so long as the third party falls under the court's personal jurisdiction and has control over the evidence.<sup>143</sup>

---

("[T]here is presently no statutory basis for the issuance of a warrant to conduct searches abroad."), *aff'd in part, vacated in part, and remanded*, 552 F.3d 157 (2d Cir. 2008).

138. See FED. R. CRIM. P. 41(b)(1).

139. *Id.* 41(b)(5) (permitting out-of-district warrants to conduct searches in U.S. territories overseas and on the premises of diplomatic or consular missions in foreign states); see *id.* advisory committee's note to 2008 amendment ("The rule is intended to authorize a magistrate judge to issue a search warrant in any of the locations for which 18 U.S.C. § 7(9) provides jurisdiction."); see also 18 U.S.C. § 7 (2015) (defining the special maritime and territorial jurisdiction of the United States); cf. Note, *Criminal Jurisdiction over Civilians Accompanying American Armed Forces Overseas*, 71 HARV. L. REV. 712, 712 n.5 (1958) (noting that at the time, there were no treaties providing consent other than Status of Forces Agreements and that the "United States can exercise jurisdiction over its civilians within a foreign territory only with the sovereign's prior consent"). For an excellent treatment of the extraterritorial aspects of U.S. criminal enforcement jurisdiction under Status of Forces Agreements, see JOSEPH M. SNEE & A. KENNETH PYE, STATUS OF FORCES AGREEMENTS AND CRIMINAL JURISDICTION 92-109 (1957).

140. See FED. R. CRIM. P. 17(c)(1); see also *Subpoena*, BLACK'S LAW DICTIONARY (10th ed. 2014) (defining a "subpoena" as a "writ or order commanding a person to appear before a court or other tribunal, subject to a penalty for failing to comply," and defining a "subpoena duces tecum" as an order requiring a person "to appear in court and to bring specified documents, records, or things").

141. See *supra* note 133.

142. See, e.g., *In re Grand Jury Proceedings the Bank of N.S.*, 740 F.2d 817, 832 (11th Cir. 1984).

143. See, e.g., *id.* at 826-28 (ordering production of evidence despite Cayman Island bank secrecy laws); *In re Grand Jury Subpoena Directed to Marc Rich & Co.*, 707 F.2d 663, 665, 670 (2d Cir. 1983) (affirming an order to produce evidence despite a claim that it would violate Swiss law); *United States v. Vetco Inc.*, 691 F.2d 1281, 1286-87 (9th Cir. 1981) (ordering production despite possible criminal penalties under Swiss law); *In re Grand Jury Subpoena Served upon Simon Horowitz*, 482 F.2d 72, 79-80 (2d Cir. 1973)

*footnote continued on next page*

Courts applying this principle have observed that “the operation of foreign law ‘do[es] not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that [law].”<sup>144</sup>

In the digital context, the steps of indirect collection are much the same as in the physical world.<sup>145</sup> For example, law enforcement may apply for court orders requiring U.S.-based providers to disclose digital evidence in their possession.<sup>146</sup> The recipient of such orders may comply by providing the requested evidence. If she does not comply and cannot show good cause, she may face judicial enforcement in the form of civil contempt sanctions.<sup>147</sup>

---

(Friendly, J.) (upholding in part a subpoena requiring an accountant to produce the contents of three locked file cabinets belonging to a client); *Columbia Pictures Indus. v. Bunnell*, No. CV 06-1093FMCJCX, 2007 WL 2080419, at \*11-12 (C.D. Cal. May 29, 2007) (ordering a party to produce digital evidence stored on servers in the Netherlands, despite the fact that doing so would violate Dutch privacy law); *United States v. Chase Manhattan Bank*, 584 F. Supp. 1080, 1086-87 (S.D.N.Y. 1984) (requiring production despite a Hong Kong judge’s bank secrecy order).

144. *Linde v. Arab Bank*, 706 F.3d 92, 109 (2d Cir. 2013) (alterations in original) (quoting *Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court*, 482 U.S. 522, 544 n.29 (1987)).

145. See COMPUT. CRIME & INTELLECTUAL PROP. SECTION, CRIMINAL DIV., U.S. DEP’T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 134 (n.d.), <http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf> [hereinafter CCIPS GUIDELINES] (“[I]nvestigators ordinarily do not themselves search through the provider’s computers in search of the materials described in the warrant. Instead, investigators serve the warrant on the provider as they would a subpoena, and the provider produces the material specified in the warrant.”). The operational trajectory is the same as the subpoena process. First, the court order is obtained. Second, the ISP is served with the order. Third, the third-party service provider gives law enforcement responsive evidence. See Orin S. Kerr, *A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1222-24 (2004) (citing 18 U.S.C. §§ 2702-2703, 2711) (describing the steps of using the Stored Communications Act (SCA) to collect digital evidence).

146. Depending on the type of information an order seeks, law enforcement is required to show varying levels of suspicion. See Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn’t*, 97 NW. U. L. REV. 607, 620 tbl.2, 621 (2003) (describing “the continuum of court orders and legal processes” that the SCA uses to govern law enforcement collection of digital evidence); see also CCIPS GUIDELINES, *supra* note 145, at 127 (“Thus, a 2703(d) court order can compel everything that a subpoena can compel (plus additional information), and a search warrant can compel the production of everything that a 2703(d) order can compel (and then some).”).

147. Recently, the Second Circuit held that, as a matter of statutory interpretation, compelled disclosure of digital evidence under the SCA, a thirty-year-old statute, does not apply to customer data stored outside the United States. See *In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197, 201 (2d Cir. 2016), *reh’g en banc denied*, No. 14-2985, 2017 WL 362765 (2d Cir. Jan. 24, 2017). However, such extraterritoriality would be consistent with the U.S. Constitution and international law’s bounds on enforcement jurisdiction, as would use of a grand

*footnote continued on next page*

Critical to criminal procedure's compliance with international norms, the United States is not authorized to "enforce its laws against an individual content provider from another country unless the content provider has a local presence."<sup>148</sup> Indeed, congressionally enacted enforcement mechanisms for indirect collection are territorial; the courts may order forfeiture only of domestic property.<sup>149</sup>

Collection of foreign-located data using compulsory process complies with international law's restrictions on enforcement jurisdiction so long as the enforcement mechanisms are limited to persons and property within the United States.<sup>150</sup> By leveraging the threat of territorial enforcement (for instance, through an order authorizing seizure of property upon a finding of contempt), law enforcement is able to require companies to produce foreign-located evidence.<sup>151</sup> The United States takes no direct extraterritorial acts when it compels disclosures and receives information despite the fact that the motivating factor for the third party is the threat of U.S. (territorial) enforcement.<sup>152</sup> All acts taken on foreign soil—including retrieval of foreign-stored information and its transport to the United States—are performed by a third party.<sup>153</sup>

---

jury subpoena to seek the same customer data stored outside the United States. *See infra* notes 150-53 and accompanying text.

148. Goldsmith, *supra* note 118, at 485.

149. When a court enters such orders, it exercises territorial enforcement jurisdiction. *See* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 431 cmt. b (AM. LAW INST. 1987). Law enforcement authorities, too, exercise enforcement jurisdiction in executing such orders. *Id.* cmt. c.

150. *Cf. In re* Petition of Boehringer Ingelheim Pharm., Inc., 745 F.3d 216, 218 (7th Cir. 2014) (Posner, J.) (noting that foreign nationals outside U.S. territory are beyond the court's subpoena power).

151. *Id.* at 216-18.

152. In a case involving a U.S. discovery order relating to French witnesses and documents, the court found that the order did not intrude on French sovereignty or judicial custom. *Adidas (Can.) Ltd. v. S.S. Seatrain Bennington*, Nos. 80 Civ. 1911 (PNL), 82 Civ. 0375 (PNL), 1984 WL 423, at \*2 (S.D.N.Y. May 30, 1984). The court concluded:

No adverse party will enter on French soil to gather evidence (or otherwise). No oath need be administered on French soil or by a French judicial authority.

What is required . . . on French soil is certain acts preparatory to the giving of evidence. [The company] must select appropriate employees to give depositions in the forum state; likewise it must select the relevant documents which it will reveal to its adversaries in the forum state. These acts do not call for French judicial participation. . . . In no way do those acts affront or intrude on French sovereignty.

*Id.*; *see also In re Anschuetz & Co.*, 754 F.2d 602, 611 (5th Cir. 1985) (concluding that a district court's ordering of depositions to be conducted on German soil was not a violation of international law).

153. *Adidas (Can.)*, 1984 WL 423, at \*2; *accord In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 15 F. Supp. 3d 466, 476 (S.D.N.Y. 2014) (holding that an order for compelled process "places obligations only on the

*footnote continued on next page*

## B. Failure of the Existing Rules

The harmony<sup>154</sup> between conventional evidence-gathering methods and international law's restrictions on extraterritorial enforcement jurisdiction begins to unravel with the practice of network investigative techniques on the dark web. The amendment to Rule 41 governing search warrant venue requirements did little more than remove a procedural hurdle in the way of courts' ability to issue warrants for territorial law enforcement searches and seizures.<sup>155</sup> In applying the legal process for search warrants to network investigative techniques, law enforcement and courts assume that anonymized targets are territorially located during all stages of implementation and enforcement.<sup>156</sup> After all, courts lack constitutional and statutory authority to issue extraterritorial warrants, and any such warrant would have no force in a foreign state without an agreement to the contrary.<sup>157</sup>

Application of the existing rules to anonymized targets results in a bizarre structural arrangement: the courts have no authority over the extraterritorial aspect of network investigative techniques, yet the issuance of search warrants is a condition precedent to their execution. Network investigative techniques that wind up targeting computers in the territorial United States are authorized by warrant, while those that land overseas draw authority directly

---

service provider to act"), *rev'd, vacated, and remanded*, 829 F.3d 197 (2d Cir. 2016), *reh'g en banc denied*, No. 14-2985, 2017 WL 362765 (2d Cir. Jan. 24, 2017).

154. As summarized by James Crawford, U.S. courts "have taken the view that whenever activity abroad has consequences or effects within the US which are contrary to local legislation then the American courts may make orders requiring the . . . production of documents." CRAWFORD, *supra* note 125, at 479-80 ("Such orders may be enforced by action within the US against individuals or property present within [U.S.] territorial jurisdiction . . .").
155. See Memorandum from David Bitkower, Deputy Assistant Att'y Gen., U.S. Dep't of Justice, to Judge Reena Raggi, Chair, Advisory Comm. on Rules of Criminal Procedure 2 (Oct. 20, 2014), in ADVISORY COMM. ON CRIMINAL RULES, *supra* note 32, at 133, 134 ("What our proposal would accomplish is untying the hands of law enforcement when it is not yet known whether the Fourth Amendment requires a warrant because it is unknown whether the media is in the United States—and it accomplishes that by ensuring that a judge is available to hear the warrant application.").
156. For example, one application requested and was granted a warrant to infect every computer that associated with a server located in Virginia. See *United States v. Michaud*, No. 3:15-cr-05351-RJB, 2016 WL 337263, at \*4 (W.D. Wash. Jan. 28, 2016). The location listed on the warrant application was Virginia, even though it authorized over 8000 malware infections of computers located in 120 countries. Cox, *FBI Hack*, *supra* note 27 ("As far as is publicly known, these mass hacking techniques have been limited to child pornography investigations. But with the changes to Rule 41, there is a chance US authorities will expand their use to other crimes too.").
157. See *United States v. Curtiss-Wright Exp. Corp.*, 299 U.S. 304, 318 (1936).

from the executive's plenary powers to enforce the laws of the United States<sup>158</sup> and from statutes authorizing the DOJ and FBI to investigate individuals for violations of U.S. laws.<sup>159</sup>

As for intra-agency checks and balances, the DOJ's existing protocols on cross-border investigations cannot be applied before the deployment of network investigative techniques on the dark web because investigators are unable to discern a target's location until after it has been hacked. For example, investigators are required to "use reasonable efforts to ascertain whether any pertinent computer system, data, witness, or subject is located in a foreign jurisdiction" and "follow the policies and procedures set out by their agencies for international investigations" to gather evidence located overseas.<sup>160</sup> These procedures typically include consultation with the DOJ's Computer Crime and Intellectual Property Section (CCIPS)—the DOJ's technology section—or the

---

158. This would require finding that pursuant to the constitutional command to "take Care that the Laws be faithfully executed," U.S. CONST. art. II, § 3, "the President has the power to authorize agents of the executive branch to engage in law enforcement activities in addition to those provided by statute," *Auth. of the FBI to Override Int'l Law in Extraterritorial Law Enf't Activities*, 13 Op. O.L.C. 163, 176 (1989). Whether the mechanics of such authority violate the separation of powers is beyond the scope of this Article. For the purposes of this Article, I concede the claim that the Take Care Clause, in conjunction with the broad authorizing statutes carrying into execution core executive powers, gives the President raw authority to make these decisions and to delegate them to nonappointed members of the DOJ. *See Auth. of the FBI*, 13 Op. O.L.C. at 176. The 1989 Office of Legal Counsel opinion effectively overruled an opinion from 1980, which concluded that the FBI may not conduct extraterritorial apprehensions in violation of international law. *See Extraterritorial Apprehension by the FBI*, 4B Op. O.L.C. 543, 549 (1980).

159. *See* 18 U.S.C. § 3052 (2015); 28 U.S.C. § 533(1) (2015). The question whether by enacting these statutes Congress delegated authority to the DOJ and the FBI to violate international law has not been addressed by the courts and is beyond the scope of this Article. Under *Chevron*, "[i]f . . . the court determines Congress has not directly addressed the precise question at issue, . . . the question for the court is whether the agency's answer [here, that it has authority to violate international law] is based on a permissible construction of the statute." *Chevron U.S.A. Inc. v. Nat. Res. Def. Council, Inc.*, 467 U.S. 837, 843 (1984). Scholars disagree regarding the extent of the deference owed the executive branch in the context of ambiguous statutory authority. *Compare* Eric A. Posner & Cass R. Sunstein, *Chevronizing Foreign Relations Law*, 116 YALE L.J. 1170, 1220 (2007) (arguing that with respect to the Authorization for Use of Military Force passed by Congress in September 2001, "the President should be taken to have the authority to interpret ambiguities as he chooses"), *with* Derek Jinks & Neal Kumar Katyal, *Disregarding Foreign Relations Law*, 116 YALE L.J. 1230, 1236 (2007) (rejecting enhanced judicial deference in foreign affairs in the "executive constraining zone").

160. ONLINE INVESTIGATIONS WORKING GRP., U.S. DEP'T OF JUSTICE, ONLINE INVESTIGATIVE PRINCIPLES FOR FEDERAL LAW ENFORCEMENT AGENTS 62 (1999) (bolding omitted). The guidelines note "the difficulties inherent in ascertaining physical location in an online environment" and instruct law enforcement agents to "seek guidance if they suspect a transborder issue may arise." *Id.* at 63.

OIA<sup>161</sup> and often require written approval before using unilateral compulsory measures for information located overseas.<sup>162</sup> However, if investigators lack knowledge of a target's location, they cannot effectively use these procedures.

In the regulatory vacuum that results, rank-and-file officers have discretion that may shape U.S. policy regarding which crimes trigger the use of cross-border network investigative techniques, the breadth of hacking techniques that are used to effectuate remote searches, and whose property may be targeted. Moreover, although the *ex ante* warrant process regulates some aspects of network investigative techniques, it does so without regard to national security or international norms. A warrant may impose constitutional limitations that check the intensity and breadth of hacking techniques. But cross-border cyberoperations will still be unilateral, invasive, and conducted without coordination with the agencies that lead U.S. foreign relations and national security policy.

### C. The Foreign Relations Risk of Hacking the Dark Web

Law enforcement's use of network investigative techniques on the dark web is in obvious tension with international norms. It is not clear whether (and to what extent) a particular network investigate technique runs afoul of international law or how targeted states may respond. This uncertainty gives rise to five categories of risk: (1) the risk of attribution, (2) the risk of vulnerability disclosure, (3) diplomatic risks associated with unauthorized cross-border operations, (4) the risk of foreign prosecution targeting U.S. law enforcement members, and (5) the risk of countermeasures the injured state may be entitled to take.

#### 1. The risk of attribution

The risk of attribution faced by investigators for cross-border network investigative techniques is heightened due to the FBI's operational protocols and the public nature of the criminal justice system. For example, in a recent case the government was ordered to disclose information about thousands of

---

161. See CCIPS GUIDELINES, *supra* note 145, at 57-58; OFFICES OF THE U.S. ATT'YS, U.S. ATTORNEYS' MANUAL § 9-13.500 (1997) (requiring prosecutors to seek approval from the OIA when seeking any assistance abroad or taking "any act outside the United States relating to a criminal investigation or prosecution").

162. See OFFICES OF THE U.S. ATT'YS, *supra* note 161, § 9-13.525 ("[A]ll Federal prosecutors must obtain written approval through the Office of International Affairs (OIA) before issuing any subpoenas to persons or entities in the United States for records located abroad."). The U.S. Attorneys' Manual and departmental policy guidance instruct prosecutors on when and how to make a request for approval and assistance from the OIA.

computers located in over a hundred foreign countries.<sup>163</sup> This requirement conflicted with defense and intelligence policy mandating secrecy for cross-border cyberoperations.

This dynamic introduces an asymmetry against the United States: U.S. attribution of harmful attacks to states is based on circumstantial evidence that is typically not definitive (and thus of questionable legitimacy, particularly when faced with denial by the accused country), whereas attribution to the United States of cross-border network investigative techniques is much more defensible because it is more likely to be based on official documents.<sup>164</sup>

The attribution issue was highlighted by the November 2014 breach at Sony Pictures Entertainment by a group calling themselves the “Guardians of Peace.”<sup>165</sup> In December 2014, the FBI attributed the hack to the North Korean government.<sup>166</sup> In its attribution, the FBI cited malware linked “to other malware that the FBI knows North Korean actors previously developed” in a 2013 attack of South Korean banks and media outlets.<sup>167</sup> Additionally, the agency noted “significant overlap between the infrastructure used in this attack and other malicious cyber activity the U.S. government has previously linked directly to North Korea.”<sup>168</sup> However, experts critical of this attribution correctly note that the evidence is not definitive.<sup>169</sup> Further fueling speculation, officials have not revealed specifics as to how they determined North Korea was responsible, likely due to the involvement of the National Security Agency (NSA) and consequent classification of the information.<sup>170</sup>

---

163. See Transcript of Evidentiary Hearing at 39, *United States v. Tippens*, No. CR16-5110RJB (W.D. Wash. Nov. 1, 2016); Cox, *FBI Hack*, *supra* note 27.

164. Without evidence of attribution satisfying the reasonable doubt standard, for example, the United States would not be able to prosecute a state actor alleged to have violated U.S. law by hacking into a computer in the United States.

165. The FBI, in its investigation, noted that the breach “consisted of the deployment of destructive malware and the theft of proprietary information as well as employees’ personally identifiable information and confidential communications. The attacks also rendered thousands of [Sony]’s computers inoperable, forced [Sony] to take its entire computer network offline, and significantly disrupted the company’s business operations.” Press Release, FBI, Update on Sony Investigation (Dec. 19, 2014), <https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation>.

166. *Id.*

167. *Id.*

168. *Id.*

169. See, e.g., Bruce Schneier, *We Still Don’t Know Who Hacked Sony*, ATLANTIC (Jan. 5, 2015), <http://www.theatlantic.com/international/archive/2015/01/we-still-dont-know-who-hacked-sony-north-korea/384198>; see also David E. Sanger & Michael S. Schmidt, *More Sanctions on North Korea After Sony Case*, N.Y. TIMES (Jan. 2, 2015), <http://nyti.ms/1ygfNOV>.

170. See Sanger & Schmidt, *supra* note 169.

## 2. The risk of vulnerability disclosure

The use of network investigative techniques also raises national security risks related to the use and disclosure of software vulnerabilities. A “zero-day” vulnerability is a software bug for which no patch exists.<sup>171</sup> Malicious code exploiting zero-day vulnerabilities can propagate from one computer to the next with impunity.<sup>172</sup> Zero-day exploits are valuable because owning a zero-day exploit, in principle, provides the capability to penetrate any device in the world running the affected software until the developer rolls out a software update that patches the security flaw.<sup>173</sup>

Intelligence agencies, whose mandate includes protecting the nation’s cyberinfrastructure from attack, generally have a greater interest in vulnerability disclosure.<sup>174</sup> To be sure, intelligence agencies also have an interest in exploiting vulnerabilities to accomplish intelligence-gathering objectives through cross-border hacking—which they no doubt value more than law enforcement interests.<sup>175</sup> However, the intelligence community has

- 
171. Andrea Peterson, *Why Everyone Is Left Less Secure When the NSA Doesn't Help Fix Security Flaws*, WASH. POST (Oct. 4, 2013), <http://wpo.st/sGT42>. The name reflects the number of days such a bug has been known to the software developer. See Kim Zetter, *Turns Out the US Launched Its Zero Day Policy in Feb 2010*, WIRED (June 26, 2015, 9:48 AM), <https://www.wired.com/2015/06/turns-us-launched-zero-day-policy-feb-2010>. See generally Jason Healy, *The U.S. Government and Zero-Day Vulnerabilities: From Pre-Heartbleed to Shadow Brokers*, J. INT'L AFF. (Nov. 1, 2016), [https://jia.sipa.columbia.edu/online-articles/healey\\_vulnerability\\_equities\\_process](https://jia.sipa.columbia.edu/online-articles/healey_vulnerability_equities_process) (criticizing the FBI's decision to contract with an undisclosed firm to unlock the iPhone used by San Bernardino shooter Syed Farook).
172. See Ryan Gallagher, *Cyberwar's Gray Market Should the Secretive Hacker Zero-Day Exploit Market Be Regulated?*, SLATE (Jan. 16, 2013, 9:00 AM), [http://www.slate.com/articles/technology/future\\_tense/2013/01/zero\\_day\\_exploits\\_should\\_the\\_hacker\\_gray\\_market\\_be\\_regulated.html](http://www.slate.com/articles/technology/future_tense/2013/01/zero_day_exploits_should_the_hacker_gray_market_be_regulated.html); Andy Greenberg, *New Dark-Web Market Is Selling Zero-Day Exploits to Hackers*, WIRED (Apr. 17, 2015, 6:25 AM), <https://www.wired.com/2015/04/therealdeal-zero-day-exploits>; Andrea Peterson, *A Company That Sells Hacking Tools to Governments Just Got Hacked*, WASH. POST (July 6, 2015), <http://wpo.st/cQT42>.
173. Tom Gjelten, *In Cyberwar, Software Flaws Are a Hot Commodity*, NPR (Feb. 12, 2013, 3:25 AM ET), <https://n.pr/WVasXe>; see Vlad Tsyркlevich, *Hacking Team: A Zero-Day Market Case Study*, TSYRKLEVICH.NET (July 22, 2015), <https://tsyркlevich.net/2015/07/22/hacking-team-0day-market>.
174. See Malena Carollo, *Influencers: Lawsuits to Prevent Reporting Vulnerabilities Will Chill Research*, CHRISTIAN SCI. MONITOR (Sept. 29, 2015), <http://fw.to/sI9NwEJ>; see also Jack Detsch, *Influencers Oppose Expanding Federal Hacking Authorities*, CHRISTIAN SCI. MONITOR (May 9, 2016), <http://passcode.csmonitor.com/influencers-rule41> (describing how, in a survey of experts from across the government, the technology and security industry, and the privacy advocacy community, “[n]early two-thirds of Passcode’s Influencers said [U.S.] judges should not be able to issue search warrants for computers located outside their jurisdictions”).
175. See David E. Sanger, *Obama Lets N.S.A. Exploit Some Internet Flaws, Officials Say*, N.Y. TIMES (Apr. 12, 2014), <http://nyti.ms/1gmYqOm>.

more sophisticated hacking capabilities than law enforcement and can therefore be much more selective about the vulnerabilities it withholds for intelligence gathering.<sup>176</sup> By contrast, law enforcement agencies have an interest in keeping a larger pool of vulnerabilities unpatched in order to use hacking techniques in pursuit of criminal suspects. The conflict has played out before the White House Vulnerabilities Equities Process—an administrative proceeding before an Equities Review Board chaired by the National Security Council—which the FBI has been criticized for bypassing entirely.<sup>177</sup>

The government's use of malware also risks exposing these vulnerabilities to criminals or malicious state actors. When a criminal or foreign agent accesses a computer hacked by the United States, he may be able to reverse-engineer the attack in order to use it to attack cyberinfrastructure in the United States.<sup>178</sup> In May 2016, software maker Mozilla filed a motion asking the FBI to disclose a potential vulnerability in the Firefox browser that the FBI allegedly used to hack visitors of a child pornography site,<sup>179</sup> “trigger[ing] a fierce debate around the responsibility of governments to disclosure [sic] vulnerabilities used in investigations to affected companies.”<sup>180</sup> The software maker underscored the cybersecurity implications of the vulnerability, arguing in its motion to intervene that “the security of millions of individuals using Mozilla's Firefox Internet browser could be put at risk by a premature disclosure of this vulnerability.”<sup>181</sup>

In a recent case the government was ordered to disclose its hacking tools' source code to the defense, but its compliance with the order was blocked by the FBI, which asserted that disclosure of the vulnerability information would

---

176. *See id.*

177. *See* Healy, *supra* note 171.

178. Amy Zegart, *Vladimir Putin Is Trying to Hack the Election: What Should US Do?*, CNN (Oct. 24, 2016, 12:18 PM ET), <http://cnn.it/2exPWwu> (“Many cyber weapons have a ‘use it and lose it’ quality. Once they are in the wild, they can be reverse engineered and possibly used against us.”).

179. Mozilla's Motion to Intervene or Appear as Amicus Curiae in Relation to Government's Motion for Reconsideration of Court's Order on the Third Motion to Compel at 1-2, *United States v. Michaud*, No. 15-CR-05351-RJB (W.D. Wash. May 11, 2016) [hereinafter Mozilla's Motion to Intervene]; Joseph Cox, *Mozilla Urges FBI to Disclose Potential Firefox Security Vulnerability*, MOTHERBOARD (May 12, 2016, 12:26 AM), <http://motherboard.vice.com/read/mozilla-urges-fbi-to-disclose-firefox-security-vulnerability>.

180. Cox, *supra* note 179.

181. Mozilla's Motion to Intervene, *supra* note 179, at 1-2 (“To protect the safety of Firefox users, and the integrity of the systems and networks that rely on Firefox, Mozilla requests that the Court order that the Government disclose the exploit to Mozilla at least 14 days before any disclosure to the Defendant, so Mozilla can analyze the vulnerability, create a fix, and update its products before the vulnerability can be used to compromise the security of its users' systems by nefarious actors.”).

have subjected the United States to national security risk.<sup>182</sup> At least one court has found that the refusal to disclose an exploit to the defense requires the suppression of any evidence obtained as a result of the technique.<sup>183</sup>

### 3. The risk to diplomatic legitimacy

The United States has an interest in taking a leadership role in norm development in cyberspace.<sup>184</sup> Harmonization between states is facilitated through diplomacy.<sup>185</sup> Hard diplomacy is the negotiation of treaties and other formal agreements.<sup>186</sup> It functions through formal, traditional channels of negotiation between the officials of two or more states or through an international organization like the United Nations. Soft diplomacy relies on indirect influence through interactions with civilians and government actors.<sup>187</sup> According to Joseph Nye, a state's soft power turns on "its culture (in places where it is attractive to others), its political values (when it lives up to

---

182. See Charlie Osborne, *FBI Refuses to Release Tor Exploit Details, Evidence Thrown out of Court*, ZDNET (May 26, 2016, 9:55 GMT), <http://zd.net/1sc15XX> ("There are 1,200 cases pending against alleged visitors to the website and the formal refusal of evidence gained by tracking these visitors could destroy the FBI's hopes of winning these cases. Without being able to submit evidence that each defendant viewed or downloaded child abuse images, many—if not all—of these cases are at risk of collapse.").

183. See Order Denying Dismissal & Excluding Evidence at 1, *Michaud*, No. 3:15-CR-05351-RJB (W.D. Wash. May 25, 2016); see also Osborne, *supra* note 182.

184. The Department of Defense (DoD) Strategy for Operating in Cyberspace states:

Given the dynamism of cyberspace, nations must work together to defend their common interests and promote security. DoD's relationship with U.S. allies and international partners provides a strong foundation upon which to further U.S. international cyberspace cooperation. Continued international engagement, collective self-defense, and the establishment of international cyberspace norms will also serve to strengthen cyberspace for the benefit of all.

U.S. Dep't of Def., Department of Defense Strategy for Operating in Cyberspace 2 (2011), <http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf>.

185. See Jack Goldsmith, *Unilateral Regulation of the Internet: A Modest Defence*, 11 EUR. J. INT'L L. 135, 146 (2000) ("When regulatory conflict and regulatory spillover occur with respect to 'real-space' transnational transactions, nations have responded with a variety of international harmonization strategies.").

186. See *id.* ("Sometimes harmonization takes the 'hard' form of treaties that either establish a uniform international standard, or an international anti-discrimination regime, or an international choice-of-law regime. Other times harmonization takes 'softer' forms like information sharing among enforcement agencies or informally agreed-upon regulatory targets.").

187. Cf. JOSEPH S. NYE, JR., *THE FUTURE OF POWER* 83 (2011) (noting the difficulties of incorporating soft power into a government's strategy because its instruments "are not fully under the control of governments," its outcomes are more in the control of the targeted state rather than the initiating state, and the results take a long time).

them at home and abroad), and its foreign policies (when others see them as legitimate and having moral authority).<sup>188</sup>

Soft power is particularly useful in the cyberspace context because of attribution and enforcement difficulties. Therefore, the public scope and nature of cross-border cyberoperations may have heightened foreign policy consequences. This is where leading by example comes into play.<sup>189</sup> As Harold Koh has argued, the “process of visibly obeying international norms builds U.S. ‘soft power,’ enhances its moral authority, and strengthens U.S. capacity for global leadership.”<sup>190</sup> It follows that the extent of the visible violations of our obligations to other nations—and our interpretation of those obligations—signals to the international community the United States’ position as to what the existing norms permit and, more broadly, sends a significant message as to the United States’ position on the rule of law.

The United States has taken the position that applying existing international norms to cyberspace is merely a matter of “applying old questions to the latest developments in technology.”<sup>191</sup> Where there are many gaps in the application of existing law to new technologies,<sup>192</sup> the United States may have an interest in nudging norm development one way or another.<sup>193</sup> Yet the

---

188. *Id.* at 84.

189. *Cf.* *United States v. Verdugo-Urquidez*, 494 U.S. 259, 285 (1990) (Brennan, J., dissenting) (“Mutuality also serves to inculcate the values of law and order. By respecting the rights of foreign nationals, we encourage other nations to respect the rights of our citizens. Moreover, as our Nation becomes increasingly concerned about the domestic effects of international crime, we cannot forget that the behavior of our law enforcement agents abroad sends a powerful message about the rule of law to individuals everywhere.”).

190. Harold Hongju Koh, *On American Exceptionalism*, 55 STAN. L. REV. 1479, 1480 (2003); *see id.* at 1480 n.2 (“Soft power rests on the ability to set the agenda in a way that shapes the preferences of others. . . . If I can get you to *want* to do what I want, then I do not have to force you to do what you do *not* want to do. If the United States represents values that others want to follow, it will cost us less to lead.” (alteration in original) (quoting JOSEPH S. NYE, JR., *THE PARADOX OF AMERICAN POWER: WHY THE WORLD’S ONLY SUPERPOWER CAN’T GO IT ALONE* 9 (2002))).

191. *See* Harold Hongju Koh, *International Law in Cyberspace*, Remarks to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), in 54 HARV. INT’L L.J. ONLINE 1, 8 (2012).

192. *See* Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L.J. 317, 335-52 (2015) (explaining the limitations of analogizing cyberspace to the high seas, outer space, or Antarctica for the purpose of applying existing legal norms).

193. *See* Henry Farrell, Council on Foreign Relations, *Promoting Norms for Cyberspace 1* (2015), [http://i.cfr.org/content/publications/attachments/Norms\\_CyberBrief.pdf](http://i.cfr.org/content/publications/attachments/Norms_CyberBrief.pdf); James Andrew Lewis, Ctr. for Strategic & Int’l Studies, *Liberty, Equality, Connectivity: Transatlantic Cybersecurity Norms 1* (2014), [https://csis-prod.s3.amazonaws.com/s3fs-public/legacy\\_files/files/publication/140225\\_Lewis\\_TransatlanticCybersecurityNorms.pdf](https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/140225_Lewis_TransatlanticCybersecurityNorms.pdf) (“Europe and the United States have a collective interest in the promotion of a stable international order based on the rule of law, open and equitable arrange-

*footnote continued on next page*

United States has not articulated—explicitly or implicitly through state practice—an intelligible principle that distinguishes one form of cross-border cyberexfiltration operation targeting persons or firms from the next. In this context, the use of network investigative techniques will no doubt draw criticism about the legitimacy of U.S. policy positions<sup>194</sup> and affect international efforts to regulate cyberoperations, all of which are still at an embryonic stage.<sup>195</sup>

By allowing rank-and-file officials to control how hacking warrants are executed, the existing legal process effectively allows the circumstances of the immediate investigation to dictate foreign policy interests in cultivating soft power. Decisionmaking at the rank-and-file level is driven by the immediate goals of a domestic criminal investigation as opposed to broader, more complex foreign policy goals. Primary decisionmaking lacks meaningful interagency coordination and is enforced by a judiciary whose umpiring capabilities are limited to preserving individual rights in the domestic sphere and who lack technological expertise to spot irregularities.<sup>196</sup>

---

ments for trade, and a commitment to democratic government and individual rights.”); see also U.S. GOV’T ACCOUNTABILITY OFFICE, GAO-10-606, UNITED STATES FACES CHALLENGES IN ADDRESSING GLOBAL CYBERSECURITY AND GOVERNANCE 1, 30, 39 (2010) (finding that the “global aspects of cyberspace present key challenges to U.S. policy”—including challenges to the United States’ ability to assert leadership in norm development, conduct interagency coordination, and pursue a consistent national strategy—and arguing that “the United States will be at a disadvantage in promoting its national interests in the realm of cyberspace” until those challenges are addressed).

194. See David E. Sanger, *Fine Line Seen in U.S. Spying on Companies*, N.Y. TIMES (May 20, 2014), <http://nyti.ms/1j6nJVq> (“China demands that the U.S. give it a clear explanation of its cybertheft, bugging and monitoring activities, and immediately stop such activity . . . .” (quoting statement from the Chinese Defense Ministry)); see also Jack Goldsmith, *The U.S. Corporate Theft Principle*, LAWFARE (May 21, 2014, 8:07 AM), <http://www.lawfareblog.com/2014/05/the-u-s-corporate-theft-principle> (“What the United States needs is an explanation convincing to audiences outside the United States about why its principle of corporate espionage is attractive beyond its furtherance of U.S. corporate and national security interests.”).

195. For example, China suspended its participation in a U.S.-China working group on cybersecurity just after the May 2014 indictments. Ting Shi & Michael Riley, *China Halts Cybersecurity Cooperation After U.S. Spying Charges*, BLOOMBERG (May 20, 2014, 2:39 AM PDT), <http://www.bloomberg.com/news/2014-05-20/china-suspends-cybersecurity-cooperation-with-u-s-after-charges.html>; see Sanger, *supra* note 194.

196. According to one former magistrate, “judges who allow technological advances to pass them by aren’t doing the public any favors by not staying current. Law enforcement has moved on, and it’s tough to act as a check against overreach if you don’t understand the subject matter.” See Tim Cushing, *Judge John Facciola on Today’s Law Enforcement: I’d Go Weeks Without Seeing a Warrant for Anything ‘Tactile,’* TECHDIRT (Mar. 3, 2015, 2:34 PM), <https://tdrt.io/exi>. And while “agents can describe the process more fully to a judge in closed chambers,” this does not occur unless “the judge knows to ask.” Ellen Nakashima, *Meet the Woman in Charge of the FBI’s Most Controversial High-Tech Tools*, WASH. POST (Dec. 8, 2015), <http://wpo.st/F2022> (attributing the statement to Amy Hess, *footnote continued on next page*

#### 4. The risk of foreign prosecution

Most, if not all, network investigative techniques that target foreign computers will violate foreign domestic law, just as foreign-launched cyberexfiltration operations would violate U.S. law,<sup>197</sup> notwithstanding a purported law enforcement purpose.<sup>198</sup> After all, a cyberexfiltration operation originating in the United States that targets a computer in another state is subject to the prescriptive jurisdiction of that state.<sup>199</sup> In 2002, for example, Russia's Federal Security Service filed criminal charges against FBI agents for remotely accessing and extracting data from servers in Chelyabinsk, Russia in order to seize evidence that was later used in a criminal trial.<sup>200</sup> The incident was reportedly "the first FBI case to ever utilize the technique of extra-territorial seizure of digital evidence."<sup>201</sup> The practice largely went underground after this incident, in part "to keep public references to [the FBI's] online surveillance tools to a minimum."<sup>202</sup> The United States, too, has prosecuted foreign state actors for hacking into computers and extracting information. More recently, the DOJ indicted five members of the Chinese military for cyberespionage.<sup>203</sup> The fact that the defendants were likely enforcing Chinese law does not change the fact that their actions violated U.S. law.

---

the head of the FBI's Operational Technology Division, which is responsible for developing and executing the FBI's network investigative techniques, and noting that judges may not really understand what they are authorizing if warrants do not describe techniques in sufficient detail).

197. See, e.g., *LVRC Holdings v. Brekka*, 581 F.3d 1127, 1130-31 (9th Cir. 2009) ("[The Computer Fraud and Abuse Act] was originally designed to target hackers who accessed computers to steal information or to disrupt or destroy computer functionality, as well as criminals who possessed the capacity to 'access and control high technology processes vital to our everyday lives. . .'" (second alteration in original) (quoting H.R. REP. NO. 98-894, at 9 (1984))).
198. Cf. *Hartford Fire Ins. Co. v. California*, 509 U.S. 764, 799 (1993) ("[T]he fact that conduct is lawful in the state in which it took place will not, of itself, bar application of the United States[] . . . laws,' even where the foreign state has a strong policy to permit or encourage such conduct." (first alteration in original) (quoting RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 415 cmt. j (AM. LAW INST. 1987))).
199. See *supra* notes 35-38 and accompanying text.
200. *Brunker*, *supra* note 42; see *United States v. Gorshkov*, No. CR00-550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001).
201. Robert Lemos, *Russia Accuses FBI Agent of Hacking*, CNET (Aug. 19, 2002, 5:05 AM PDT) (quoting FBI press release), <http://cnet.co/2IRHM6r>.
202. See *Timberg & Nakashima*, *supra* note 18 (attributing the statement to former U.S. officials).
203. See Press Release, U.S. Dep't of Justice, *supra* note 42.

The DOJ recognizes that cross-border network investigative techniques threaten the sovereignty of other nations. DOJ guidelines for online investigations warn investigators that accessing remotely stored data, or even initiating “personal contact with residents of a foreign state, may violate foreign law. In addition, activity by U.S. law enforcement in such areas may be regarded as a violation of the other nation’s sovereignty, creating the potential for serious diplomatic conflict.”<sup>204</sup> The Office of the U.S. Attorneys’ Criminal Resource Manual cautions that another “nation may regard an effort by an American investigator or prosecutor to investigate a crime or gather evidence within its borders as a violation of sovereignty,” including even “seemingly innocuous acts as a telephone call[] [or] a letter.”<sup>205</sup>

## 5. The risk of countermeasures

Affected states that perceive the use of cross-border network investigative techniques as a violation of the United States’ international law obligations may seek “self-help” in the form of countermeasures.<sup>206</sup> Countermeasures are “State actions, or omissions, directed at another State that would otherwise violate an obligation owed to that State.”<sup>207</sup> Countermeasures must be proportionate to the harm suffered and necessary to compel or convince the violating state to “desist in its own internationally wrongful acts or omissions.”<sup>208</sup>

An injured state’s right to take countermeasures is triggered by the discovery of a violation of an international norm or treaty obligation

---

204. ONLINE INVESTIGATIONS WORKING GRP., *supra* note 160, at 16; *see also* CCIPS GUIDELINES, *supra* note 145, at 58 (noting that “issues such as sovereignty and comity may be implicated” in the event investigators access “a computer located in another country” without permission).

205. OFFICES OF THE U.S. ATT’YS, CRIMINAL RESOURCE MANUAL § 267 (1997).

206. *See* Hathaway et al., *supra* note 41, at 857; Michael N. Schmitt, “*Below the Threshold*” *Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA. J. INT’L L. 697, 699 (2014) (detailing how the law of countermeasures applies to cross-border cyberoperations); *see also* Katharine C. Hinkle, *Countermeasures in the Cyber Context: One More Thing to Worry About*, 37 YALE J. INT’L L. ONLINE 11, 12 (2011) (“[R]eciprocal countermeasures—which have been cited by the U.S. Department of Defense and several scholars as being an effective and even preferable mode of self-help in the cyber context—are deeply problematic for an international legal regime that seeks to appropriately constrain state responses to cyber-conflict.” (footnote omitted)).

207. Schmitt, *supra* note 206, at 700. The Draft Articles of State Responsibility codify when and how a state is held responsible for a breach of an international obligation and how a state may respond to international law violations that fall below the threshold of an armed attack or a prohibited use of force. *See* Int’l Law Comm’n, Rep. on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10, at 56-57 (2001).

208. Schmitt, *supra* note 206, at 700.

attributable to a particular state.<sup>209</sup> Once these requirements are met, the principle of proportionality plays a central role in “modulating the escalation of conflict between states.”<sup>210</sup> In the cyber context, “[t]erritorial sovereignty protects cyber infrastructure located on a State’s territory, regardless of its governmental character, or lack thereof,”<sup>211</sup> and it may be violated “even when no damage results, as in the case of emplacement of malware designed to monitor a system’s activities.”<sup>212</sup>

As noted, it is well established that direct exercise of one state’s law enforcement functions in the territory of another state requires that state’s consent.<sup>213</sup> States that attribute cross-border network investigative techniques to the United States may have a defensible claim that the United States violated customary international law’s prohibition on the extraterritorial exercise of law enforcement functions without consent<sup>214</sup> as well as the concomitant principle of nonintervention, which “forbids all States or groups of States to intervene directly or indirectly in internal or external affairs of other States.”<sup>215</sup> This is particularly the case for attributed law enforcement hacking

---

209. Hinkle, *supra* note 206, at 16 (“The threshold inquiry for evaluating the legality of countermeasures asks whether there has been (1) an internationally wrongful act that (2) is attributable to another state.”).

210. Thomas M. Franck, *On Proportionality of Countermeasures in International Law*, 102 AM. J. INT’L L. 715, 718 (2008); *see* Hinkle, *supra* note 206, at 18-20.

211. Schmitt, *supra* note 206, at 704.

212. *Id.* at 705 (distinguishing such activities from mere espionage or “monitoring,” which are permitted); *see also* Susan W. Brenner & Joseph J. Schwerha IV, *Transnational Evidence Gathering and Local Prosecution of International Cybercrime*, 20 J. COMPUTER & INFO. L. 347, 352 (2002) (arguing that direct access of foreign-located data “cannot provide the conceptual basis for approaching the legal issues involved in transborder searches and seizures because it would inevitably allow the victim state to transgress upon another state’s sovereignty by searching and seizing property belonging to that state’s citizens, property that is physically located within that state’s territorial boundaries”).

213. *See supra* notes 121-29 and accompanying text; *see also, e.g.*, Stephan Wilske & Teresa Schiller, *International Jurisdiction in Cyberspace: Which States May Regulate the Internet?*, 50 FED. COMM. L.J. 117, 171 (1997) (“Enforcement measures requiring consent include not only the physical arrest of a person, but also, for example, service of subpoena, orders for production of documents, and police inquiries.”).

214. *See* Bellia, *supra* note 35, at 77 n.143 (concluding that cross-border cyberexfiltration operations violate customary international law based on “the notion that a foreign country’s manipulation of data is akin to a trespass and to interference with protected privacy interests”). *But see* Jack L. Goldsmith, *The Internet and the Legitimacy of Remote Cross-Border Searches*, 2001 U. CHI. LEGAL F. 103, 108 (arguing that logging on to a remote server after lawfully acquiring a target’s password credentials is territorially “ambiguous” and may therefore be in compliance with customary international law).

215. *Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.)*, Judgment, 1986 I.C.J. Rep. 14, ¶ 205, at 107-08 (June 27); *see Corfu Channel (U.K. v. Alb.)*, Judgment, 1949 I.C.J. Rep. 4, 35 (Apr. 9).

operations that move forward with a search after the initial intrusion despite learning that the target is located overseas. Interference with property interests distinguishes network investigative techniques from other forms of espionage, such as the use of spy satellites, where State A's personnel and instruments are anchored in a jurisdictionally neutral territory (for example, outer space) and therefore do not violate the territorial integrity of State B.<sup>216</sup>

A review of applicable treaties and diplomatic communications reveals that no state has consented to the United States' launch of cross-border network investigative techniques. In fact, the only multilateral agreement to address the issue of law enforcement "remote access" directly—the Council of Europe's Convention on Cybercrime (Budapest Convention)—explicitly refused to authorize remote cross-border searches.<sup>217</sup> As Oona Hathaway noted, the Budapest Convention may "limit the extent to which parties to the Convention could conduct cyber-attacks against other state parties, since that would undermine the overall intent of the agreement."<sup>218</sup> In 1995, Council of Europe ministers tasked with considering the legal implications of cross-border network investigative techniques recommended against the practice.<sup>219</sup> Experts commissioned in 2009 by the Council of Europe's Project on Cybercrime explained:

The Recommendation reflects the common understanding of the drafters that investigative activity of law enforcement authorities of a State Party in international communication networks or in computer systems located in the territory of another state may amount to a violation of territorial sovereignty of the state

- 
216. See Bellia, *supra* note 35, at 77 n.143 ("[I]nterference with property interests—as well as personal privacy interests—distinguishes a remote cross-border search from other activities, such as the use of satellites for remote sensing related to management of natural resources and environmental protection, that are not thought to violate international law.").
217. See Convention on Cybercrime, *opened for signature* Nov. 23, 2004, S. TREATY DOC. NO. 108-11 (2006), 2296 U.N.T.S. 167 (entered into force July 1, 2004) [hereinafter Budapest Convention]. The Budapest Convention was ratified by the U.S. Senate in September 2006. *Chart of Signatures and Ratifications of Treaty 185*, COUNCIL EUR., <https://go.coe.int/Be71y> (last visited Apr. 4, 2017).
218. Hathaway et al., *supra* note 41, at 864.
219. Comm. of Ministers, Council of Eur., Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology (1995), <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76>. Duncan Hollis has argued that the Budapest Convention's drafters may have purposefully left open provisions concerning cyberattacks by law enforcement. See Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1052 (2007).

concerned, and therefore cannot be undertaken without prior consent of the State concerned.<sup>220</sup>

The use of countermeasures to respond to a cyberattack is illustrated by the U.S. response to North Korea's hack of Sony. After the attacks on Sony, President Obama made a public statement that the United States would "respond proportionately" to the incident, calling it an act of cybervandalism.<sup>221</sup> Just days later, the North Korean Internet experienced outages for about ten hours.<sup>222</sup> Many, including North Korea, speculated that the United States was behind a hack that resulted in the outages.<sup>223</sup> That day, Marie Harf, a State Department spokeswoman, told reporters, "We aren't going to [publicly] discuss . . . operational details about the possible response options. . . . [A]s we implement our responses, some will be seen, some may not be seen."<sup>224</sup>

Further complicating the matter is the lack of consensus among states as to how to classify cross-border cyberoperations. As Matthew Waxman notes, "[i]t is widely believed that sophisticated cyber attacks could cause massive harm—whether to military capabilities, economic and financial systems, or social functioning—because of modern reliance on system interconnectivity."<sup>225</sup> And because states differ in how they interpret the application of international norms to harmful cyberoperations, "there is a range of reasonable interpreta-

- 
220. See Henrik W.K. Kaspersen, *Cybercrime and Internet Jurisdiction* 26 (2009), <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803042b7> (explaining that the use of processing capacity or data stored on computer systems in a state encroaches on that state's territorial sovereignty, despite uncertainty as to whether cross-border activity in the form of mere communication, such as via telephone, violates territorial sovereignty). In light of this concern, the Convention's drafters agreed to allow direct unilateral cross-border access to data only when those data were generally accessible or when explicit consent was obtained from the data's owner or custodian. See *Budapest Convention*, *supra* note 217, art. 32. In this sense, article 32 is "a permissive rule derived from international custom or from a convention." See *S.S. Lotus (Fr. v. Turk.)*, Judgment, 1927 P.C.I.J. (ser. A) No. 10, at 19 (Sept. 7).
221. David Jackson, *Obama: We're Not at Cyberwar with North Korea*, USA TODAY (Dec. 21, 2014, 1:17 PM EST), <http://usat.ly/16FuBL2>.
222. See Brian Fung, *North Korea's Internet Outage Was Likely the Work of Hacktivists—But Not the Ones You Might Think*, WASH. POST (Dec. 23, 2014), <https://wpo.st/6dwd2>.
223. See Jack Kim, *North Korea Blames U.S. for Internet Outages, Calls Obama "Monkey"*, REUTERS (Dec. 28, 2014, 2:40 AM EST), <http://reut.rs/1EwYeNF>; see also Ashley Feinberg, *So Who Shut Down North Korea's Internet?*, GIZMODO (Dec. 23, 2014, 3:50 PM), <http://gizmodo.com/so-who-shut-down-north-koreas-internet-1674589139>.
224. See Nicole Perlroth & David E. Sanger, *North Korea Loses Its Link to the Internet*, N.Y. TIMES (Dec. 22, 2014), <https://nyti.ms/1ARmSCL>. A week later the United States placed sanctions on three organizations and ten individuals associated with the North Korean government. See *Sony Cyber Attack: North Korea Calls US Sanctions Hostile*, BBC NEWS (Jan. 4, 2015), <http://www.bbc.com/news/world-asia-30670884>.
225. Matthew C. Waxman, *Self-Defensive Force Against Cyber Attacks: Legal, Strategic and Political Dimensions*, 89 INT'L L. STUD. 109, 109 (2013).

tions of cyber ‘armed attacks’ for the purposes of triggering militarily forceful self-defense, and a stable consensus is unlikely for the foreseeable future.”<sup>226</sup>

The U.S. position on the use of force in cyberspace incorporates the “scale and effects” test, which focuses on the consequences of a cyberoperation.<sup>227</sup> While this is the most widely held view,<sup>228</sup> a competing position turns on the status of the target and privileges “critical infrastructure” with special protected status.<sup>229</sup> Yet another position turns on the “instrumentality theory,” where “[t]he more analogous a new weapon is to conventional forms of military force, the more likely its operation will constitute a ‘use of force’ or ‘armed attack.’”<sup>230</sup>

According to the Senate Armed Services Committee,

experts agree that gaining access to a target for intelligence collection is tantamount to gaining the ability to attack that target. If a penetration were detected,

---

226. *Id.* at 120-21. Testifying before the Senate Committee considering his nomination to lead the NSA and United States Cyber Command, Michael Rogers explained:

As a matter of law, DoD believes that what constitutes a use of force in cyberspace is the same for all nations, and that our activities in cyberspace would be governed by Article 2(4) of the U.N. Charter the same way that other nations would be. With that said, there is no international consensus on the precise definition of a use of force, in or out of cyberspace. Thus, it is likely that other nations will assert and apply different definitions and thresholds for what constitutes a use a [sic] force in cyberspace, and will continue to do so for the foreseeable future.

Advance Questions for Vice Admiral Michael S. Rogers, USN: Nominee for Commander, United States Cyber Command 11-12 (2014) [hereinafter Advance Questions], [http://www.armed-services.senate.gov/imo/media/doc/Rogers\\_03-11-14.pdf](http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf). For an extensive discussion of the debate surrounding the definition of “force” and “armed attack” in Articles 2(4) and 51 of the U.N. Charter, see generally Waxman, *supra* note 41, at 431-37.

227. As Michael Rogers explained:

DoD has a set of criteria that it uses to assess cyberspace events. As individual events may vary greatly from each other, each event will be assessed on a case-by-case basis. While the criteria we use to assess events are classified for operational security purposes, generally speaking, DoD analyzes whether the proximate consequences of a cyberspace event are similar to those produced by kinetic weapons.

Advance Questions, *supra* note 226, at 11.

228. See Hathaway et al., *supra* note 41, at 847 (“Steering a middle course between the instrument- and target-based views, the effects-based approach is the most promising and most widely accepted approach.”).

229. One problem with this “target-based” approach is that states define “critical infrastructure” in different ways. See TENACE, CRITICAL INFRASTRUCTURE PROTECTION: THREATS, ATTACKS AND COUNTERMEASURES 5-8 (2014), [http://www.dis.uniroma1.it/~tenace/download/deliverable/Report\\_tenace.pdf](http://www.dis.uniroma1.it/~tenace/download/deliverable/Report_tenace.pdf) (distinguishing between definitions in the European Union and in the United States); cf. Waxman, *supra* note 41, at 436 (discussing the target-based approach).

230. Reese Nguyen, Comment, *Navigating Jus ad Bellum in the Age of Cyber Warfare*, 101 CALIF. L. REV. 1079, 1117 (2013).

the victim may not know whether the purpose of the activity would be limited to espionage only, or would also constitute preparation for an attack.<sup>231</sup>

This, coupled with the doctrinal uncertainties described above, may increase the risk of escalation by victim states under the purported justification of anticipatory self-defense, upon a (mistaken, though defensible) fear of an attack in the proximate future. It is for this reason that when Rogers was asked if there were classes of overseas targets that should be “‘off-limits’ from penetration through cyberspace,”<sup>232</sup> he explained that “the U.S. Government should only conduct cyberspace operations against carefully selected foreign targets that are critical to addressing explicitly stated intelligence and military requirements, as approved by national policymakers and the national command authority.”<sup>233</sup>

This appears to directly clash with the use of cyberoperations to collect evidence in pursuit of a criminal actor. Consider a case from 2012 in which an FBI agent applied for and received a warrant to use network investigative techniques to target a suspect believed to be a member of the Iranian military located in Iranian territory.<sup>234</sup> Due to a software malfunction, “the program hidden in the link sent to [the target] never actually executed.”<sup>235</sup> But what if the malfunction caused harm to the target computer? Or worse, what if the program executed successfully but allowed the Iranians to match its forensically obtained digital signature to malware used in other, more hostile attacks that were *then* attributed to the United States? In either case, it would be defensible for an adversary state to respond.

The inherent unreliability of malware adds to the risk of escalation. Malware functionality is inherently buggy, and malfunction may lead to harmful, irreversible consequences and collateral damage associated with its

---

231. See Advance Questions, *supra* note 226, at 12 (bolding omitted).

232. *Id.* at 13 (bolding omitted).

233. *Id.*

234. See Timberg & Nakashima, *supra* note 18 (noting that a photo e-mailed by the suspect to investigators “appeared to show an olive-skinned man in his late 20s, wearing what court documents described as an Iranian tan camouflaged military uniform,” and that the IP address used to register the e-mail address years prior suggested he was in Tehran, Iran). The suspect “allegedly threatened to detonate bombs at a county jail, a DoubleTree hotel, the University of Denver, the University of Texas, San Antonio International Airport, Washington-Dulles International Airport, Virginia Commonwealth University and other heavily used public facilities across the country.” *Id.* The investigators executing the warrant used a spear phishing technique and sent an e-mail containing a link that, when clicked, would cause surveillance software to be downloaded on the target machine. *Id.*; see *supra* note 108 and accompanying text (describing spear phishing techniques).

235. See Timberg & Nakashima, *supra* note 18 (quoting a handwritten note from the FBI agent to the court).

use.<sup>236</sup> For example, “[p]oorly designed malware could cause the destruction of data or the corruption of the whole operating system.”<sup>237</sup> This is only exacerbated by the Internet of Things phenomenon and the potential security risks of using interconnected devices such as smart light bulbs, connected cars, smart fridges, wearables, and other home security systems.<sup>238</sup> The FBI highlighted this very issue in a 2015 public service announcement about the safety risks associated with the Internet of Things, warning that lack of consumer awareness as to the threat exposure may allow attackers to execute online attacks, resulting in a number of risks, including *physical* harm to consumers.<sup>239</sup>

### III. Toward a Normative Legal Process

With the advent of network investigative techniques on the dark web, it has become clear that the criminal legal process should be adjusted to ensure that it better regulates government conduct that has an impact on U.S. foreign relations or national security. Rather than wait for political fallout as a precondition for government intervention,<sup>240</sup> a more forward-looking approach would reallocate decisionmaking authority to institutions better suited to identify and balance foreign relations risks against the law enforcement benefits of using cross-border network investigative techniques.<sup>241</sup>

This raises three fundamental regulatory questions: First, which institutions should set these preferences and calibrate them as the government moves forward within a complex and unpredictable global cybersecurity land-

---

236. RONALD J. DEIBERT, *BLACK CODE: INSIDE THE BATTLE FOR CYBERSPACE* 25, 31-32 (2013); Mark Mekow & Lakshmikanth Raghavan, *Security Testing of Custom Software Applications*, CSO (July 28, 2010, 8:00 AM PT), <http://www.csoonline.com/article/2125378/application-security/security-testing-of-custom-software-applications.html>; Quinn Norton, *Everything Is Broken*, MEDIUM: MESSAGE (May 20, 2014), <https://medium.com/message/everything-is-broken-81e5f33a24e1#oc3f76k26>.

237. RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R44547, *DIGITAL SEARCHES AND SEIZURES: OVERVIEW OF PROPOSED AMENDMENTS TO RULE 41 OF THE RULES OF CRIMINAL PROCEDURE* 9 (2016).

238. *See Internet of Things Poses Opportunities for Cyber Crime*, FED. BUREAU OF INVESTIGATION (Sept. 10, 2015), <https://www.ic3.gov/media/2015/150910.aspx>.

239. *Id.*

240. *Cf.* NEIL K. KOMESAR, *IMPERFECT ALTERNATIVES: CHOOSING INSTITUTIONS IN LAW, ECONOMICS, AND PUBLIC POLICY* 30-34 (1994) (noting that law and economics analysis tends to precondition government intervention on regulatory failure to satisfy efficiency benchmarks).

241. *See* Rubin, *supra* note 49, at 469 (“A more comprehensive institutional comparison might consider other goals . . .”).

scape?<sup>242</sup> Second, what policy preferences can be set (using direct and indirect government intervention) to mitigate the immediate risks caused by the failure of the existing rules? Third, how should the policy preferences be implemented and enforced, considering the comparative institutional failures of the existing system?<sup>243</sup>

This Part begins to answer these questions and in doing so outlines a preliminary legal process for managing network investigative techniques. First, it conducts a comparative institutional analysis and concludes that the executive branch is best suited to assume primary responsibility for future government hacking policy. It proposes an interagency conflict resolution scheme to ensure law enforcement hacking policy decisions do not offend foreign relations or national security interests. Second, it sets out baseline policy preferences that constrict the scope of hacking power delegated to the rank-and-file officers executing this new surveillance technique. Third, it lays out a regulatory scheme for implementation and enforcement that involves “a complex, dynamic interaction of institutions that simultaneously work together, challenge each other, defend themselves and divide responsibility.”<sup>244</sup> The objective is to enhance the ability to produce decision rules that are predictably and objectively applied, democratically legitimate, and in the overall public interest.<sup>245</sup>

#### A. Failure of the Existing Legal Process

To be sure, responsibility for the existing system’s failure does not lie with *institution-wide* incompetence on the part of the executive branch with respect to foreign relations. The existing system fails because it authorizes rank-and-file officials to make decisions that have direct foreign policy implications

---

242. Stated another way, which institutions should set rules that balance law enforcement interests against countervailing foreign relations interests? *See id.* at 469 & n.25 (“Law and economics has framed the regulatory debate as an institutional comparison; the operative question is not how well the market functions, but whether the regulatory system could produce a better outcome.” (citing RICHARD A. POSNER, *ECONOMIC ANALYSIS OF LAW* (2d ed. 1977))).

243. *See* Patricia L. Bellia, *Designing Surveillance Law*, 43 ARIZ. ST. L.J. 293, 297 (2011) (calling these “second-order” design choices for enforcing “first-order” preferences).

244. Rubin, *supra* note 49, at 467; *see* Edward L. Rubin, *The New Legal Process, the Synthesis of Discourse, and the Microanalysis of Institutions*, 109 HARV. L. REV. 1393, 1396 (1996) [hereinafter Rubin, *New Legal Process*]; *see also* Daniel B. Rodriguez, *The Substance of the New Legal Process*, 77 CALIF. L. REV. 919, 952 n.177 (1989) (book review) (arguing that “[t]he core insight of legal process is that [policy solutions] will emerge from the synergies associated with the process itself” rather than from substantive law).

245. *See* Rubin, *New Legal Process*, *supra* note 244, at 1414-16 (calling these the most accepted goals for rules).

without meaningful guidance or oversight.<sup>246</sup> This Subpart articulates an executive interagency decisionmaking framework that maximizes information, expertise, coordination, and the ability to make decisions on the fly.

As noted, courts are constrained by the territoriality of warrant authority,<sup>247</sup> broad deference to law enforcement on investigatory matters,<sup>248</sup> and broad deference to the executive branch on matters of foreign policy,<sup>249</sup> particularly in the face of statutory silence or ambiguity.<sup>250</sup> In addition, magistrate judges lack subject matter expertise regarding complex computer science questions and are therefore ill equipped to scrutinize search warrant applications that involve such technologies.<sup>251</sup>

The gap between DOJ policy and DOJ action may also suggest that rank-and-file officers, as opposed to the overarching executive branch, lack subject matter expertise in computer network security and international cyberspace law.<sup>252</sup> Stated another way, rank-and-file officers may not be properly implementing current executive branch policy for cross-border searches because they lack the requisite expertise to realize current policy is applicable in the first place.

---

246. See *supra* Part II.B.

247. See *supra* Part II.A.

248. Cf. Rachel A. Harmon, *The Problem of Policing*, 110 MICH. L. REV. 761, 776 (2012) (noting that courts are deferential to law enforcement in part because they recognize their own limited institutional competence). *But cf.* *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 587-88 (1952) (“In the framework of our Constitution, the President’s power to see that the laws are faithfully executed refutes the idea that he is to be a lawmaker.”).

249. See Curtis A. Bradley, *Chevron Deference and Foreign Affairs*, 86 VA. L. REV. 649, 651 (2000) (“Courts have given deference to the executive branch in foreign affairs matters throughout the nation’s history . . . .”); Harold Hongju Koh, *Why the President (Almost) Always Wins in Foreign Affairs: Lessons of the Iran-Contra Affair*, 97 YALE L.J. 1255, 1337 (1988) (“The courts have too readily read [United States v.] *Curtiss-Wright* [Exp. Corp., 299 U.S. 304 (1936)], as standing for the proposition that the Executive deserves an extra, and often dispositive, measure of deference in foreign affairs above and beyond that necessary to preserve the smooth functioning of the national government.” (italics omitted)).

250. See *Chevron U.S.A. Inc. v. Nat. Res. Def. Council, Inc.*, 467 U.S. 837, 842-43 (1984). Scholars disagree regarding the extent of the deference owed the executive branch in the context of ambiguous statutory authority, but there is no disagreement that some deference is required. See *supra* note 159.

251. See *supra* note 196.

252. See Robert M. Chesney, *National Security Fact Deference*, 95 VA. L. REV. 1361, 1411-12 (2009) (“Superior access to information or expertise contributes nothing to accuracy, after all, unless the decisionmaker actually exploits them, and does so reliably.”); see also *id.* at 1411 n.168 (citing RICHARD S. MARKOVITS, *MATTERS OF PRINCIPLE: LEGITIMATE LEGAL ARGUMENT AND CONSTITUTIONAL INTERPRETATION* 217 (1998) (arguing that institutional expertise should be given less weight where the officials “did not actually investigate despite their capacity to do so”)).

The executive branch—as a whole—has a comparative institutional advantage over Congress and the federal courts in terms of making foreign policy decisions that turn on rapidly changing technologies. Executive agencies such as the DOJ, the State Department, and the NSA arguably have superior systematic access to information and expertise on both foreign relations and technology—whether through their own subject matter experts<sup>253</sup> or access to other executive agencies that specialize in foreign policy, intelligence gathering, and technology capabilities.<sup>254</sup> By pooling administrative resources, the executive can configure a policymaking team that brings together information and expertise related to foreign relations, law enforcement, technology, and cybersecurity.<sup>255</sup>

An executive agency implementation scheme also has the advantage of being able to adapt in response to rapidly changing technologies and the uncertainties of international norm development. By using executive instruments to set substantive policy preferences, there is minimal cost of changing policy, facilitating a dynamic, nimble policy regime.<sup>256</sup> For example, the DOJ can more easily centralize on-the-fly decisionmaking and provide notice through the rulemaking process and a variety of other administrative

---

253. See William S. Dodge, *Extraterritoriality and Conflict-of-Laws Theory: An Argument for Judicial Unilateralism*, 39 HARV. INT'L L.J. 101, 160 (1998) (“It seems clear that the political branches are institutionally better equipped than courts to reach agreement with other nations about how international business should be regulated.”); Koh, *supra* note 249, at 1336 (noting courts’ lack of expertise and suggesting structural solutions, including centralization of the adjudication of national security claims in a particular court such as the U.S. Court of Appeals for the District of Columbia Circuit); Julian Ku & John Yoo, *Hamdan v. Rumsfeld: The Functional Case for Foreign Affairs Deference to the Executive Branch*, 23 CONST. COMMENT. 179, 199-201 (2006) (describing how the executive branch’s institutional competence in foreign relations is superior to that of the judiciary); Paul Ohm, *Electronic Surveillance Law and the Intra-Agency Separation of Powers*, 47 U.S.F. L. REV. 269, 280-83 (2012).

254. Cf. Ku & Yoo, *supra* note 253, at 195-201 (“[C]ourts have access to limited information in foreign affairs cases . . .”).

255. The team should include the Cyber Coordinator, the NSA’s representative for the vulnerability equities process, and representatives from the DOJ’s CCIPS and OIA.

256. See Neal Kumar Katyal, *Internal Separation of Powers: Checking Today’s Most Dangerous Branch from Within*, 115 YALE L.J. 2314, 2318 (2006) (“And in contrast to the doubters of the unitary executive, I believe a unitary executive serves important values, particularly in times of crisis. Speed and dispatch are often virtues to be celebrated.”); see also Elena Kagan, *Presidential Administration*, 114 HARV. L. REV. 2245, 2331-46 (2001).

mechanisms.<sup>257</sup> The DOJ also has the capacity to generate uniform rules “and to publicize those rules as binding upon the entire nation.”<sup>258</sup>

By contrast, Congress and the courts tend to be sluggish or nonuniform in their decisionmaking.<sup>259</sup> The courts can examine changing issues on a case-by-case basis, but their system of precedent and jurisdictional limitation slows the generation of decision rules that have a uniform national application. And while Congress is able to promulgate laws uniformly, it has not passed a comprehensive electronic surveillance law in over thirty years.<sup>260</sup>

On the other hand, when an institution “makes a major policy move on its own” without sufficient basis in legislative authorization, as it seems the DOJ has done with network investigation techniques, “it undercuts the democratic legitimacy of statutes.”<sup>261</sup> The use of cross-border network investigative techniques undercuts the DOJ’s democratic legitimacy to the extent it requires an interpretation of its statutory investigative authority to extend overseas, allowing rank-and-file officials to conduct cross-border investigative activities in violation of customary international law, without more explicit authorization from Congress.<sup>262</sup>

Thus, if the executive were to allot broad discretion to rank-and-file officials to shape foreign policy as a matter of course in the execution of search warrants, it would be more consistent with democratic goals to pass the policy

---

257. William N. Eskridge Jr., *Expanding Chevron’s Domain: A Comparative Institutional Analysis of the Relative Competence of Courts and Agencies to Interpret Statutes*, 2013 WIS. L. REV. 411, 419 (“[A]gencies have a variety of mechanisms that allow them to generate national rules relatively quickly: administrative rulemaking, published guidances, handbooks, and even online websites.”).

258. *Id.*

259. *Id.* (arguing that case-by-case adjudication is slow); David Alan Sklansky, *Two More Ways Not to Think About Privacy and the Fourth Amendment*, 82 U. CHI. L. REV. 223, 227 (2015) (“And while statutes theoretically can be revised at any time, without waiting for the proper case to arise and without regard for precedent, in practice Congress is often notoriously sluggish.”).

260. *Cf.* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510-2522 (2015)).

261. *See* Eskridge, *supra* note 257, at 436.

262. Such an interpretation of statutory authority runs against *the executive’s own interpretation* of FBI authority to override customary international law in extraterritorial law enforcement activities. That interpretation requires “direction of the President or the Attorney General” for the FBI to “use its statutory authority” to “investigate and arrest individuals for violations of applicable United States law” if “those actions depart from customary international law.” *Auth. of the FBI to Override Int’l Law in Extraterritorial Law Enft Activities*, 13 Op. O.L.C. 163, 183 (1989). *But cf.* *Extraterritorial Apprehension by the FBI*, 4B Op. O.L.C. 543 (1980) (finding no authority for the FBI to conduct cross-border abductions of noncitizens in violation of customary international law).

modification through Congress before it became law.<sup>263</sup> Instead, the executive should adopt the narrower scope of baseline law enforcement hacking capabilities articulated in Part III.B below, which constrain the broad hacking powers the FBI currently has without undermining immediate investigatory goals.

Expansion of law enforcement hacking powers from the baseline preferences should balance law enforcement interests with competing foreign relations and national security interests. One way to do this might be to characterize the problem as a horizontal agency conflict between the DOJ, the NSA, and the State Department. Notwithstanding details of the institutional design solution, the resolution of this conflict should ideally “take advantage of the ability of adversarial relationships to foster fuller development of information and debate, along with broader representation for conflicting interests.”<sup>264</sup> To that end, it should entail three things: First, it should balance interests and resolve the conflict. Second, it must generate and promulgate two types of information: (a) information about each agency’s policies and (b) information about technical facts. Third, it must generate a record of this information.

That being the case, there are several mechanisms the executive can use.<sup>265</sup> The President can, for example, direct the agencies to negotiate a Memorandum of Understanding (MOU) on interagency protocols that the FBI must follow (for example, decisions must be made under the advisement of the President).<sup>266</sup> The President can, alternatively, create an interagency task force that makes recommendations on law enforcement hacking policy. The President can task the White House Cybersecurity Coordinator with leading a

---

263. See Katyal, *supra* note 256, at 2317 (“[T]he Founders assumed that massive changes to the status quo required legislative enactments, not executive decrees.”). As Eskridge has noted, “[s]uch usurpation, even for the best of reasons, is inconsistent with the democratic premises of Article I, Section 7: major policy decisions need to pass through both chambers of Congress and, usually, the President before they become the law of the land.” Eskridge, *supra* note 257, at 436.

264. See Daniel A. Farber & Anne Joseph O’Connell, *Agencies as Adversaries*, 105 CALIF. L. REV. (forthcoming 2017) (manuscript at 23) (on file with author).

265. See *id.* (manuscript at 24-27) (discussing three forms of interagency conflict resolution mechanisms: resolution through negotiation, resolution through executive adjudication, and resolution through formal voting and consensus rules).

266. See *id.* (manuscript at 24) (citing examples of MOUs between agencies); see also Daphna Renan, *Pooling Powers*, 115 COLUM. L. REV. 211, 213-14 (2015) (describing an MOU between the NSA and the DHS “that brings the NSA’s technical prowess to bear on DHS-led efforts to secure [domestic] critical infrastructure,” allowing the DHS to “achieve cybersecurity objectives that, as a practical matter, would otherwise be unobtainable”).

council composed of a high-ranking member of each agency.<sup>267</sup> These decisionmaking frameworks maximize information, expertise, coordination, and the ability to make decisions in response to a rapidly shifting global cybersecurity terrain.

## B. Substantive Policy Preferences

This Subpart prescribes substantive restrictions to deal with the immediate risks posed by cross-border network investigative techniques. It identifies three areas where regulation may provide solutions to the new facts of network investigative techniques and proposes standards that balance law enforcement interests against foreign policy interests. To that end, the following substantive policy preferences are not in and of themselves meant to set the normative thresholds for the use of network investigative techniques.<sup>268</sup> Rather, the restrictions are meant to provide a “baseline” from which the executive can craft policy decisions that balance the law enforcement interest in solving criminal cases against the foreign policy and national security interests of the United States. The overriding goal in prescribing them is to minimize the risks outlined in Part II.C above, leaving open the possibility for diplomatic overtures, without forgoing the pressing investigatory needs of locating criminal actors on the dark web.

### 1. What hacking techniques should be authorized?

A search warrant broadly permits investigators to “use remote access to search electronic storage media and to seize or copy electronically stored information.”<sup>269</sup> There is no discernable limit to the range of hacking activities a warrant authorizes. The scope of information that may be collected from

---

267. This representation is meant to articulate a balance among law enforcement, national security, and diplomatic interests. Of course, the President can add members to this committee or modify their roles. For example, the process can be made more autonomous, in that decisions to expand the government’s cross-border hacking policies can be made by a two-thirds vote of the committee, which would ensure balance between law enforcement interests and those of foreign policy and national security. A requirement that the Attorney General sign off on policy changes would allow the DOJ to effectively veto changes that reduce law enforcement hacking capabilities below the baseline policy preferences described in Part III.B below.

268. The normative goal of these “baseline” prescriptions is thus to facilitate prospective policymaking by minimizing the potential harm that rank-and-file decisions can cause to the negotiation processes integral to soft and hard harmonization efforts, the risk of retaliation by other nations, and potential disclosure conflicts between law enforcement and the intelligence community. Importantly, the following policy preferences are not meant to set a “ceiling” on government hacking powers but rather a “floor” from which policy can flow.

269. See FED. R. CRIM. P. 41(b)(6).

foreign-located devices by law enforcement can be limited to location information, unless consent is provided from the host nation or custodian of the target device.<sup>270</sup> Such a modification to the scope of law enforcement hacking power satisfies the central investigatory goal of “locating” the target computer while minimizing the interference with the foreign state’s sovereignty.<sup>271</sup>

In most cases, country information can be deciphered from IP address information and then used to determine whether the investigation should move forward. If the investigation target is domestic, investigators can proceed with more intrusive means. If the target ends up being overseas, the investigator can initiate the existing diplomatic protocols for cross-border collection of digital evidence, such as the MLAT process.<sup>272</sup> This solution would direct agents to make reasonable efforts to determine the location of digital evidence being remotely collected and to proceed using diplomatic protocols in the event it becomes known during the course of a search that the data are located overseas. It complies with the DOJ’s current implementation guidelines and is therefore predictable.<sup>273</sup>

---

270. This rule would comply with norms set by the Budapest Convention. *See* Budapest Convention, *supra* note 217, art. 32 (permitting cross-border access to stored computer data if the data are publicly available or if law enforcement has first obtained consent from the owner of the device). This rule would also comply with U.S. electronic surveillance laws. *See* 18 U.S.C. § 2511(2)(d) (2015); *United States v. Barone*, 913 F.2d 46, 49 (2d Cir. 1990) (permitting the recording of a conversation between A defendant and a government informant, provided the government obtains the informant’s consent and cooperation); *Shefts v. Petrakis*, 758 F. Supp. 2d 620, 630 (C.D. Ill. 2010) (noting that the collection of e-mails and text messages is permitted with consent).

271. Collection of publicly available port information does not infringe international law. *See* Budapest Convention, *supra* note 217, art. 32. Moreover, a solution that only returns country information is of sufficiently low intensity that proportionate responses by injured states are unlikely to be prohibitive. *See supra* notes 227-35 and accompanying text.

272. *See supra* Part I.B.

273. *See* ONLINE INVESTIGATIONS WORKING GRP., *supra* note 160, at 64 (“[A]gents should always make reasonable efforts to find out where the relevant electronic records are stored. If they learn before or during the search that the information may be stored in servers outside the United States, they must proceed as they would to obtain physical evidence located outside the U.S. If agents later discover they have inadvertently downloaded information from servers located abroad, they should seek immediate guidance from those authorities within their agencies who handle obtaining evidence from foreign nations.”).

2. Who should be targeted?

The Federal Rules of Criminal Procedure allow investigators to search and seize the property of nonsuspects.<sup>274</sup> International law, on the other hand, requires a proper prescriptive basis—some nexus between the search target and the harmful local effects that spawned the investigation in the first place—before a state may exercise any form of extraterritorial jurisdiction.<sup>275</sup>

Operationally, the use of network investigative techniques risks hacking foreign-located computers that belong to innocent people. One potential baseline policy preference that strikes the balance is to require investigators to make a showing of *target* culpability—for example, that the target device is owned or controlled by a criminal suspect or a fugitive.<sup>276</sup> Another way to strike this balance is to limit the use of cross-border network investigative techniques to the collection of items whose mere possession violates U.S. law.<sup>277</sup> These limiting principles minimize the situations where the United States asserts jurisdiction over a foreign-located noncitizen who has not caused effects in the United States, thus making cross-border network investigative techniques more defensible to the international community.

3. What crimes should trigger use of hacking techniques?

Another factor that will likely affect how states react to encroachments on their sovereignty that result from cross-border network investigative techniques is the seriousness of the crime being investigated. As noted, international norms in cyberspace are in development and likely to emerge as a result of state practice. The DOJ has made it clear that it intends to use hacking techniques for all crimes, regardless of the potential cross-border implications.<sup>278</sup>

---

274. See FED. R. CRIM. P. 41(c) (providing that a warrant may issue for “evidence of a crime,” “contraband . . . or other items illegally possessed,” or “property designed for use, intended for use, or used in committing a crime”).

275. See *supra* notes 35-38 and accompanying text (describing the effects test for prescriptive jurisdiction).

276. Cf. *United States v. Grubbs*, 547 U.S. 90, 96 (2006) (“Anticipatory warrants are, therefore, no different in principle from ordinary warrants. They require the magistrate to determine (1) that it is *now probable* that (2) contraband, evidence of a crime, or a fugitive *will be* on the described premises (3) when the warrant is executed.”).

277. Network investigative techniques that infect computers that visit a particular child pornography server are particularly effective in sting operations because anyone who knowingly accesses the server is committing a crime. See Memorandum from Jonathan J. Wroblewski, Dir., Office of Policy & Legislation, Criminal Div., U.S. Dep’t of Justice, to Judge John F. Keenan, Chair, Subcommittee on Rule 41, Advisory Comm. on Rules of Criminal Procedure (Jan. 17, 2014), in ADVISORY COMM. ON CRIMINAL RULES, *supra* note 25, at 179, 180, 205-06.

278. See *id.*

The DOJ's position would make it defensible for foreign law enforcement actors to hack computers in the United States as long as those actors are in investigatory pursuit of a violation of that foreign nation's criminal laws. This is a policy decision that should benefit from the experience and expertise of other agencies and consideration of U.S. foreign relations and national security implications.

There are several ways to reduce the scope of crimes that trigger the use of hacking techniques. One baseline policy preference might limit the use of network investigative techniques to counterterrorism investigations, for which—at least under the United States' interpretation of international law—extraterritorial enforcement is grounded in conceptions of self-defense.<sup>279</sup>

Another limiting principle that would likely be defensible with U.S. allies in the international community is one that tailors the use of network investigative techniques to the pursuit of crimes whose seriousness is broadly acknowledged by states, such as terrorism, child pornography offenses, drug crimes, and organized cybercrime.<sup>280</sup> Indeed, there is a history of coordination among the Group of Eight (G8) countries with regard to regulating these crimes.<sup>281</sup> For these reasons, cross-border action limited to a small set of crimes considered especially heinous will be perceived as more reasonable than an open-ended solution and thus may be more likely to receive the support of the international community.<sup>282</sup> This solution will cause minimal friction with allies, and it is therefore more likely to keep diplomatic channels open.<sup>283</sup>

---

279. The legality of such actions is not always certain. See David Kretzmer, *Targeted Killing of Suspected Terrorists: Extra-Judicial Executions or Legitimate Means of Defence?*, 16 EUR. J. INT'L L. 171, 191-97 (2005) (arguing that in international armed conflicts suspected terrorists are not combatants, though in noninternational armed conflicts they may well be combatants, and arguing that the applicable system should incorporate features of both international human rights law and international humanitarian law).

280. See Bert-Jaap Koops & Morag Goodwin, *Cyberspace, the Cloud, and Cross-Border Criminal Investigation: The Limits and Possibilities of International Law* 74 (Tilburg Law Sch. Legal Studies Research Paper Series, No. 05/2016, 2014), <https://ssrn.com/abstract=2698263>.

281. See Goldsmith, *supra* note 185, at 147 ("The G8 economic powers have recently begun to coordinate regulatory efforts concerning Internet-related crimes in five areas: paedophilia and sexual exploitation; drug-trafficking; money laundering; electronic fraud, such as theft of credit-card numbers, and computerized piracy; and industrial and state espionage.").

282. See *id.* at 147-48 (suggesting that there will be more cross-border coordination of regulatory efforts in areas where national interests converge).

283. An even less risk-averse approach may allow the use of cross-border network investigative techniques to be triggered by all crimes with extraterritorial application, satisfying the requirements of prescriptive jurisdiction though still subjecting the United States to some level of risk. One advantage of the executive branch promulgating these policy preferences is the ability to create and change policy on the fly. See *supra* note 256. This facilitates a law enforcement policy that is in tune with foreign relations policies on cyberspace, which are largely set by the executive.

### C. Implementation and Enforcement

Having selected the institutional actors that should set substantive cross-border hacking policy preferences for law enforcement moving forward, this Subpart turns to the implementation and enforcement of those policies. The existing disparity between DOJ policy and practice suggests a breakdown in implementation and enforcement.<sup>284</sup> This inconsistency “undermines the predictability of law and reverses assumptions upon which private industry and the public sector have reasonably relied.”<sup>285</sup>

The judiciary is the traditional regulating institution for criminal procedure.<sup>286</sup> Its neutrality and detachment make it suitable to make the inferences required to grant or deny a warrant<sup>287</sup> in light of the obvious conflict of interest presented by law enforcement’s focus on the “often competitive enterprise of ferreting out crime.”<sup>288</sup> Ex ante judicial review helps prevent investigators from ignoring or misinterpreting the established legal limits on their authority.<sup>289</sup> Ex post judicial review provides additional checks that incorporate the adversarial process. However, the courts are constrained in their authority to regulate cross-border aspects of network investigative techniques because of warrant authority’s territoriality, the compulsion to defer to law enforcement, and judicial deference to the executive in the realm of foreign policy.<sup>290</sup> This leaves Congress as the primary interbranch check on the foreign relations implications of law enforcement hacking.

Congress can influence the legal process in a number of ways without legislating substantively. First, Congress could legislate procedural

---

284. See Katyal, *supra* note 256, at 2318. Jonathan Mayer notes the following implementation problems with network investigative techniques: (1) “[d]escriptions of malware are often ambiguous and misleading,” (2) investigators sometimes “assert[] that no warrant is required at all,” (3) malware may be delivered to innocent users, (4) “[w]arrant applications [may] ignore . . . the unambiguous[] time limits of Rule 41,” and (5) “the government [may] not properly appl[y] for a super-warrant in scenarios where they are unambiguously required.” Jonathan Mayer, *Constitutional Malware* 75 (Nov. 15, 2016) (unpublished manuscript), <https://ssrn.com/abstract=2633247>.

285. See Eskridge, *supra* note 257, at 436.

286. See, e.g., *Johnson v. United States*, 333 U.S. 10, 14 (1948).

287. *Id.*

288. *Id.* The structure of the Fourth Amendment recognizes the intransigence of this conflict by requiring a neutral disinterested arbiter to make the determination of what is a search and whether the executive has shown probable cause of a crime sufficient to overcome the constitutional privacy interest of the target. See U.S. CONST. amend. IV; *Johnson*, 333 U.S. at 14.

289. S. REP. NO. 90-1097, at 97 (1968) (“Judicial review of the decision to intercept wire or oral communications will not only tend to insure that the decision is proper, but it will also tend to assure the community that the decision is fair.”).

290. See *supra* notes 247-51.

mechanisms that encourage predictable, objective application of government hacking policies and clear and accountable lines of command within the executive branch. For example, Congress could enact a statutory requirement that any warrant application for the use of network investigative techniques on the dark web must be authorized by the U.S. Attorney General or another designated high-ranking official.<sup>291</sup> Limiting the government actors who may authorize the application for a hacking warrant “centralizes in a publicly responsible official subject to the political process the formulation of law enforcement policy on the use of electronic surveillance techniques.”<sup>292</sup> Having high-ranking officials sign off on individual warrants increases the concentration of information and expertise in the decisionmaking process<sup>293</sup> and incentivizes applications only where the circumstances justify them.<sup>294</sup> Such a requirement would avoid the development of divergent practices across the U.S. Attorneys’ Offices while providing “lines of responsibility . . . to an identifiable person” in the event of abuse.<sup>295</sup> Additionally, by forcing the agency to absorb some of the costs of violating policy, this solution would incentivize restraint in execution.<sup>296</sup> Congress could also require certifications

- 
291. This requirement would mirror that for applications seeking an order to intercept wire or oral communications, which requires that “[t]he Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division or National Security Division specially designated by the Attorney General” authorize the filing of the application. 18 U.S.C. § 2516(1) (2015) (footnote omitted).
292. S. REP. NO. 90-1097, at 97; *cf.* FED. R. CRIM. P. 41(b) (permitting any federal law enforcement officer or attorney for the government to apply for a search warrant).
293. *See* Joseph Lynch, *Justice Department Procedures for Approval of Wiretapping and Eavesdropping Orders*, CRIM. DEF., Sept.-Oct. 1977, at 11, 11 (providing a description of internal review procedures for the Wiretap Act). The Wiretap Act was first passed as Title III of the Omnibus Crime Control and Safe Streets Act of 1968. *See* Wiretapping and Electronic Surveillance, Pub. L. No. 90-351, tit. III, 82 Stat. 211 (codified as amended at 18 U.S.C. §§ 2510-2522). In 1986, Congress amended the Wiretap Act to extend telephone wiretap restrictions to computer data transmissions. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510-2522).
294. *See* *United States v. Giordano*, 416 U.S. 505, 515 (1974) (noting in the context of the Wiretap Act that Congress “evinced the clear intent to make doubly sure that the statutory authority be used with restraint and only where the circumstances warrant the surreptitious interception of wire and oral communications”). The DOJ’s commentary has rejected any limitations on the scope or manner of execution. *See* Memorandum from David Bitkower to Judge Reena Raggi, *supra* note 155, at 3 (arguing against restrictions on remote search authority).
295. *See* S. REP. NO. 90-1097, at 97 (“This provision in itself should go a long way toward guaranteeing that no abuses will happen.”).
296. *See generally* Robert W. Hahn, *The Economic Analysis of Regulation: A Response to the Critics*, 71 U. CHI. L. REV. 1021 (2004) (explaining and defending cost-benefit analysis in regulatory decisionmaking).

to satisfy the judge that “normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous.”<sup>297</sup> This leverages DOJ expertise in situations where the courts lack appropriate technological expertise to assess whether the target’s location has indeed been obscured by technological means.<sup>298</sup>

Second, Congress could exercise oversight powers on federal law enforcement’s use of network investigative techniques. Congressional oversight can be implemented through legislative hearings by a standing congressional committee, such as the House Judiciary Committee or the House Intelligence Committee. To bolster the effectiveness of the oversight process, Congress should work to “equaliz[e] its access to sensitive information that otherwise lies solely within the Executive’s control” and build centralized technology and foreign affairs expertise within Congress to better analyze that information.<sup>299</sup> This can be done by passing legislation imposing reporting requirements on the scope and nature of permitted hacking techniques, their frequency of use, and instances where foreign-located computers are affected. Hearings should be open to the public to the extent possible, limiting closed sessions to cases where information that is classified or related to an ongoing investigation must be shared with members.

Third, Congress could indirectly regulate the nature and scope of hacking techniques used by investigators through its authority over financial and budgetary matters. Malware is expensive, with prices rising as high as \$500,000.<sup>300</sup> By adjusting budget allocations, for example, Congress could indirectly control law enforcement’s procurement of malware tools through line item adjustments or by barring the use of funds to procure tools that do not comply with the vulnerability equities process.

Fourth, Congress can allocate resources to bolster the judiciary’s technological expertise. The courts will continue to play a key role in regulating network investigative techniques by interpreting and applying constitutional and statutory checks and balances. These functions require, at minimum, an understanding of how the network investigative technique under scrutiny

---

297. See 18 U.S.C. § 2518(3)(c) (requiring such certifications before approving a telephone warrant request). In commentary, the DOJ has rejected such a “necessity requirement.” See Memorandum from David Bitkower to Judge Reena Raggi, *supra* note 155, at 3.

298. Cf. Ctr. for Democracy & Tech., *supra* note 31, at 6-7 (describing various instances when a target’s location may be obscured but not in a manner that stifles the use of current investigative techniques).

299. Koh, *supra* note 249, at 1327.

300. See Greenberg, *supra* note 172; see also Brian Fung, *The NSA Hacks Other Countries by Buying Millions of Dollars’ Worth of Computer Vulnerabilities*, WASH. POST (Aug. 31, 2013), <https://wpo.st/Qb2e2> (explaining that in 2013 the NSA allocated more than \$25 million to purchase malware from private parties).

works. This, in turn, requires a level of technological expertise. To that end, technology training and access to expert assistance when necessary is critical to ensure that judges can ask the right questions and spot irregularities.

Fifth, Congress could legislate mechanisms that encourage adversarial challenges to the legality of network investigative techniques. One way to do this through the courts is to enact an evidentiary suppression sanction for violations in the application or execution of network investigative techniques.<sup>301</sup> This would enable a criminal defendant to challenge the use of evidence obtained from unlawful hacking.<sup>302</sup> Statutory suppression also incentivizes restraint in execution by making law enforcement absorb the cost of a violation.<sup>303</sup> This also invites outside scrutiny of network investigative techniques, which can add valuable technical expertise to the public debate.<sup>304</sup> By ensuring that other institutions and the public have ample opportunities to review the use of this powerful tool, society can ensure that law enforcement has clear incentives to exercise reasonable care when using network investigative techniques.<sup>305</sup>

### Conclusion

Law enforcement's use of hacking techniques to pursue criminal suspects on the dark web will result in overseas cyberexfiltration operations that may violate the sovereignty of other nations. The risks associated with such techniques are enormous: disability of U.S. foreign relations, exposure of the United States and its citizens to countermeasures, and exposure of the

---

301. Statutory suppression of evidence applies in other surveillance contexts. See 18 U.S.C. § 2518(10)(a) (providing statutory suppression for persons aggrieved by a violation of the Wiretap Act); cf. Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 63 (2004) (“[O]nline surveillance, including dynamic content interceptions, lack[s] the statutory suppression remedy that Congress provided for traditional surveillance in the Wiretap Act. . . . The omission is not aligned with a major goal of the [Electronic Communications Privacy Act]—to ensure the privacy of electronic communications and extend all of the Wiretap Act’s protections to the new media.”).

302. See S. REP. NO. 90-1097, at 96 (1968) (noting that in the wiretapping context, “[s]uch a suppression rule is necessary and proper to protect privacy”). A standard that matches the Wiretap Act would allow any aggrieved person—not just those whose devices were breached—to challenge the legality of such evidence, so long as it is being used against her in a trial, hearing, or any other legal proceeding.

303. See *supra* note 296 and accompanying text.

304. One example of outside scrutiny is challenges by technical experts in criminal cases.

305. Orin S. Kerr, *Lifting the “Fog” of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 817 (2003) (explaining that wiretaps are subject to more oversight than compelled disclosure of digital evidence under the SCA because the latter lacks a statutory suppression remedy).

investigators performing overseas searches and seizures to prosecution by foreign nations. These circumstances highlight the failures of the existing rules of criminal procedure as applied to the new facts of cross-border network investigative techniques. And they call into question the wisdom of authorizing rank-and-file officials to make enforcement decisions that reverberate globally without any meaningful interagency coordination or interbranch checks and balances.

Criminal procedure must evolve to balance the use of network investigative techniques against countervailing foreign relations interests that may be harmed by unlawful foreign searches. This will require adjustments to the legal process that minimize the risk of political fallout by (1) maintaining existing jurisdictional norms governing the United States' cross-border criminal investigations and (2) implementing structural modifications that allocate critical foreign policy decisions to the government institutions best suited to make them. Only then can network investigative techniques be implemented and enforced in a way that is predictable, legitimate, and in the public interest.