PRIVACY INTERNATIONAL

Privacy International Briefing

International Human Rights Implications of Reported Mexican Government Hacking Targeting Journalists and Human Rights Defenders

28 June 2017

A. Introduction

On 19 June 2017, Citizen Lab at the University of Toronto's Munk School of Global Affairs, together with R3D, SocialTIC and Article 19 Mexico, published the results of an investigation, which indicated that Mexican authorities had used NSO Group's Pegasus spyware to target journalists and human rights defenders working to expose government corruption and human rights abuses. NSO Group is a surveillance technology company that sells products and services, including malware, exclusively to government clients. These attacks were designed to compromise the mobile phones of targeted individuals, permitting the attackers to surreptitiously turn on cameras and microphones, record calls, read messages, and track movements.

This investigation expands upon a Citizen Lab report in February 2017, which suggested that Mexican authorities had used NSO Group's Pegasus spyware to similarly target individuals involved in a high-profile "soda tax" campaign in Mexico. That report, in turn, followed a Citizen Lab report in August 2016, which indicated that United Arab Emirates ("UAE") authorities had targeted a human rights defender also using Pegasus spyware.

Following the publication of the 19 June 2017 report, victims of the spyware campaign have called for an independent inquiry by an international team of experts. In addition, nine of the victims have filed a criminal complaint with the office of the Attorney General of Mexico. On 22 June 2017, President Enrique Peña Nieto acknowledged that the Mexican government had purchased the NSO Group's Pegasus spyware but denied involvement in the attacks against journalists and human rights defenders.

As discussed below, Mexican government hacking, including the use of NSO Group spyware, raises grave human rights concerns and calls into question whether Mexico is meeting its obligations under international human rights law. Privacy International therefore urges Mexican authorities to immediately cease all hacking activities. We further support the calls by the victims for an independent inquiry and call on the Attorney General's Office to conduct a prompt, thorough and independent investigation of the criminal complaint.

In addition, Privacy International and R3D make the following further recommendations.

To the President of the United Mexican States to:

- Make public what hacking activities Mexican authorities have undertaken to date and by which authorities, including avowing the reported use of NSO Group spyware against journalists, human rights defenders and activists;
- Clarify the Mexican government's understanding of the legal basis for its hacking activities and what rules and safeguards, if any, regulate its hacking activities;

- Confirm what types of hacking tools, including malware, are employed by Mexican authorities and how the acquisition and use of these technologies is regulated and monitored.

To the Attorney General's Office, the General Congress of the United Mexican States, the National Human Rights Commission, the Mechanism to Protect Human Rights Defenders and Journalists, and the National Institute for Transparency, Access to Information and Personal Data Protection to:

- Conduct prompt, thorough and independent investigations into:
    - The nature and scope of government hacking activities, including whether such activities are compliant with international and domestic law;
    - The reported use of NSO Group spyware against journalists, human rights defenders and activists, with a view to bringing to justice the perpetrators and providing redress to the victims of these abuses;
    - The types of hacking tools, including malware, employed by Mexican authorities and whether their acquisition and use are compliant with international and domestic law.
- Make publicly available any findings related to the above investigations.

To all Mexican authorities that are conducting or have conducted hacking activities to:

- Notify all targets of their hacking activities to date, indicating the purported legal basis and relevant rules, if any, governing such activities;
- Destroy all material obtained through their hacking activities;
- Provide all targets of their hacking activities with an avenue for redress.

B. Background

1. NSO Group

NSO Group is one of over 520 surveillance technology companies identified by Privacy International that sells products and services exclusively to government clients for law enforcement and intelligence-gathering purposes.[1] NSO Group was founded in 2010 in Israel. Francisco Partners, a U.S.-based private equity fund, currently owns a controlling stake in the company after purchasing it for a reported U.S. $120 million in 2014.[2]

According to a promotional brochure, NSO Group describes itself as a "leader in the field of Cyber warfare . . . [working] with military and homeland security organizations in order to

[1] Privacy International, *The Global Surveillance Industry*, July 2016, available at https://www.privacyinternational.org/node/911.
[2] Joseph Cox & Lorenzo Franchesci-Bicchierai, *Meet NSO Group, The New Big Player In The Government Spyware Business,* 25 Aug. 2016, available at https://motherboard.vice.com/en_us/article/nso-group-new-big-player-in-government-spyware.

enhance their technological abilities in both the offensive and defensive cyber warfare arenas."[3] The brochure further notes that Pegasus – the spyware suite used to target journalists, human rights defenders and activists in Mexico – is "a powerful and unique monitoring tool . . . [w]hich allows remote and stealth monitoring and full data extraction from remote target devices via untraceable commands."

2. Documented Attacks Involving NSO Group Spyware

a. UAE Human Rights Defender Ahmed Mansoor

In August 2016, Citizen Lab published the results of an investigation, which indicated that UAE authorities had targeted Ahmed Mansoor, a prominent human rights defender, using NSO Group's Pegasus spyware.[4] Mr. Mansoor had received suspicious text messages with links purporting to contain information about the torture of UAE citizens.[5] Upon examination, Citizen Lab discovered that the links belonged to "an exploit infrastructure connected to NSO Group" and "led to a chain of zero-day exploits ("zero-days") that would have remotely jailbroken Mr. Mansoor's stock iPhone 6 and installed sophisticated spyware."[6] That spyware, had it infected Mr. Mansoor's phone, would have permitted UAE authorities to secretly turn on his camera and microphone, record his calls, log messages sent and received in his chat apps, and track his movements. Citizen Lab notified Apple of its findings, which resulted in Apple's release of the iOS 9.3.5 patch, which fixes the vulnerabilities exploited by the NSO Group as part of the targeting of Mr. Mansoor.[7]

On 20 March 2017, Mr. Mansoor was arrested by UAE authorities and currently remains in detention facing speech-related charges that include using social media websites to "publish false information that harms national unity."[8] On 28 March 2017, a group of United Nations human rights experts called on the UAE government to release Mr. Mansoor immediately, describing his arrest as "a direct attack on the legitimate work of human rights defenders in the UAE."[9] On 20 April 2017, a coalition of 20 human rights organizations similarly called

---

[3] NSO Group promotional brochure, available at https://sii.transparencytoolkit.org/docs/NSO-Group_Pegasus_Brochuresii_documents.

[4] Bill Marczak & John Scott-Railton, *The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender*, 24 Aug. 2016, available at https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/ [hereinafter *Million Dollar Dissident*]; *see also* Nicole Perlroth, *iPhone Users Urged to Update Software After Security Flaws Are Found*, N.Y. Times, 25 Aug. 2016, available at https://www.nytimes.com/2016/08/26/technology/apple-software-vulnerability-ios-patch.html [hereinafter *iPhone Users Urged*].

[5] Mr. Mansoor has been targeted in the past using government-exclusive spyware. In 2011, he was targeted with FinFisher's FinSpy, and in 2012, he was targeted with Hacking Team's Remote Control System. *See Million Dollar Dissident*, *supra*.

[6] *See id.* A "zero day" exploits a vulnerability that is unknown to the software or hardware manufacturer.

[7] *See iPhone Users Urged*, *supra*.

[8] Amnesty International, *UAE: Free Prominent Rights Defender Ahmed Mansoor Held on Speech-Related Charges*, 20 Apr. 2017, https://www.amnesty.org/en/documents/mde25/6094/2017/en/.

[9] Office of the U.N. High Commissioner for Human Rights, *UN rights experts urge UAE: "Immediately release Human Rights Defender Ahmed Mansoor*," 28 Mar. 2017, available at http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21449&LangID=E.

on the UAE government to release Mansoor immediately as "the charges against him relate to his human rights work and his criticism of the authorities."[10]

As part of its investigation into the use of NSO Group spyware to target Mr. Mansoor, Citizen Lab also uncovered evidence of other individuals who may have been targeted with the same government-exclusive spyware.[11] One of those potential targets was Mexican journalist Rafael Cabrera, who had recently broken a story on conflicts of interest involving the Mexican President and First Lady.

b. Mexican Public Health Researchers and Advocates

In February 2017, Citizen Lab published the results of an investigation, which suggested that Mexican authorities had used NSO Group's Pegasus spyware to target individuals involved in a high-profile "soda tax" campaign in Mexico.[12] These attacks targeted at least three individuals: Dr. Simon Barquera, a researcher at the Mexican National Institute for Public Health (INSP); Alejandro Calvillo, Director at El Poder del Consumidor; and Luis Manuel Encarnación, Coordinator of the ContraPESO Coalition. Dr. Barquera is a well-respected scientist working on nutrition policy and Mr. Calvillo and Mr. Encarnación are public health advocates whose respective organizations focus on obesity and soda consumption in Mexico. All three were prominent supporters of Mexico's 2014 soda tax, which aims to reduce national consumption of beverages that include added sugar.

Citizen Lab's report revealed that the NSO exploit infrastructure and spyware discovered in its prior investigation of the links sent to Mr. Mansoor were also used to target Dr. Barquera, Mr. Calvillo and Mr. Encarnación. The timing of the links coincided with the launch of a campaign by public health researchers and organizations – including Dr. Barquera, Mr. Calvillo and Mr. Encarnación – to double the soda tax.[13] As with the prior attack on Mr. Mansoor, these attacks were designed to compromise the phones of these individuals, permitting the attackers to surreptitiously turn on cameras and microphones, record calls, read messages and track movements.[14]

c. Mexican Journalists and Human Rights Defenders

On 19 June 2017, Citizen Lab, together with R3D, SocialTIC and Article 19 Mexico, published the results of an investigation, which indicated that Mexican authorities had used

---

[10] Human Rights Watch, *UAE: Free Prominent Rights Defender, Ahmed Mansoor Held on Speech-Related Charges*, 20 Apr. 2017, available at https://www.hrw.org/news/2017/04/20/uae-free-prominent-rights-defender.
[11] *Million Dollar Dissident*, *supra*.
[12] John Scott-Railton et al., *Bitter Sweet: Supporters of Mexico's Soda Tax Targeted with NSO Exploit Links*, 11 Feb. 2017, available at https://citizenlab.org/2017/02/bittersweet-nso-mexico-spyware/ [hereinafter *Bitter Sweet*]; *see also* Nicole Perlroth, *Spyware's Odd Targets: Backers of Mexico's Soda Tax*, N.Y. Times, 11 Feb. 2017, available at https://www.nytimes.com/2017/02/11/technology/hack-mexico-soda-tax-advocates.html [hereinafter *Spyware's Odd Targets*].
[13] *See Spyware's Odd Targets*, *supra*.
[14] *See Bitter Sweet*, *supra.*

NSO Group's Pegasus spyware to target journalists and human rights defenders working to expose government corruption and human rights abuses.[15] This report expanded upon its February 2017 report describing similar attacks targeting supporters of Mexico's "soda tax" campaign.

The most heavily targeted individual was Carmen Aristegui, a prominent investigative reporter and founder of *Aristegui Noticias*, an outlet that has broken numerous major stories on government scandals, including the 2014 Casa Blanca investigation.[16] Ms. Aristegui received 26 text messages containing links and purporting to come from a variety of sources, including the U.S. Embassy in Mexico, AMBER Alerts, her bank, and colleagues.[17] Ms. Aristegui's son was also separately targeted with over 21 messages, several also impersonating the U.S. Embassy or containing information relating to his mother.

The attacks targeted a number of other journalists, including Sebastián Barragán, a journalist working with *Aristegui Noticias*; Carlos Loret de Mola, a *Televisa* anchor; and Salvador Camarena and Daniel Lizárraga, both reporters specializing in anti-corruption investigations with Mexicanos Contra la Corrupción y la Impunidad (Mexicans against Corruption and Impunity). Mr. Camarena and Mr. Lizárraga have also previously worked with *Aristegui Noticias*.[18]

The attacks also targeted individuals working at Centro Miguel Agustin Pro Juárez ("Centro PRODH") and Instituto Mexicano para la Competitividad ("IMCO": Mexican Institute for Competitiveness). Centro PRODH is one of Mexico's most well-respected human rights organizations and represents victims of government human rights abuses, including the families of 43 students who went missing in the city of Iguala in September 2014. IMCO is a Mexican NGO whose work includes anti-corruption policy and advocacy. At Centro PRODH, the attacks targeted the Director, Mario Patrón, and two lawyers, Santiago Aguirre and Stephanie Brewer. At IMCO, they targeted the Director, Juan Pardinas, and an investigator, Alexandra Zapata.

---

[15] John Scott-Railton et al., *Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware*, 19 June 2017, available at https://citizenlab.org/2017/06/reckless-exploit-mexico-nso/ [hereinafter *Reckless Exploit*]; *see also* Article 19, R3D, SocialTIC, *Gobierno Espía: Vigilancia sistemática a periodistas y defensores de derechos humanos en México*, 19 June 2017, available at https://r3d.mx/2017/06/19/gobierno-espia/; Azam Ahmed & Nicole Perlroth, *Using Texts as Lures, Government Spyware Targets Mexican Activists and Their Families*, N.Y. Times, 19 June 2017, available at https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html?ref=nyt-es&mcid=nyt-es&subid=article.

[16] The Casa Blanca investigation concerned the construction of a multi-million dollar home by a government contractor for the family of the Mexican President. *See* Jo Tuckman, *Mexican president Enrique Peña Nieto faces outcry over £4.4m mansion*, The Guardian, 10 Nov. 2014, available at https://www.theguardian.com/world/2014/nov/10/mexico-president-enrique-pena-nieto-mansion-explain.

[17] *See Reckless Exploit*, *supra*.

[18] Citizen Lab's August 2016 report on the use of NSO Group spyware to target UAE human rights defender Ahmed Mansoor also uncovered evidence that Rafael Cabrera, a journalist working with *Aristegui Noticias* (now with *BuzzFeed*), may have also been targeted by the spyware. *See Million Dollar Dissident*, *supra*.

Citizen Lab's report connects the NSO exploit infrastructure and spyware discovered in its prior investigations with links sent to the individuals described above.[19] The timing of these links coincided with high-profile investigations into government corruption or commission of human rights abuses between January 2015 and August 2016. For example, the targeting of *Aristegui Noticias* journalists maps onto the period when they were working on uncovering the 2014 Casa Blanca scandal. The targeting of Mr. Loret corresponds with the period when he was reporting on extrajudicial killings on a farm known as "Rancho El Sol." And the targeting of staff at Centro PRODH coincides with the period just before the organization was set to make a public announcement regarding findings related to the 43 disappeared students. As with the prior attempted attacks on Mr. Mansoor and the Mexican "soda tax" advocates, these attacks were designed so the attackers could access a range of information stored on the victims' phones and to facilitate intrusive real-time surveillance.

C. The Privacy Implications of Government Hacking

Hacking has the potential to be far more intrusive than any other existing surveillance technique, including the interception of communications. Hacking permits governments remote access to devices and therefore potentially to all of the information stored on those devices. For an increasing number of individuals, personal digital devices contain the most private information they store anywhere, replacing and consolidating address books, physical correspondence, journals, filing cabinets, photo albums and wallets.

Hacking also permits governments to conduct novel and grave forms of real-time surveillance. Through hacking, a government can potentially capture continuous screenshots of the hacked device or see anything typed into that device, including login details and passwords, internet browsing histories, and draft documents and communications the user never intended to disseminate. Hacking also permits governments to covertly turn on a device's microphone, webcam and GPS-based locator technology.

By controlling the functionality of systems, hacking can even potentially permit governments to delete data or recover data that has been deleted. Hacking also permits governments to corrupt or plant data, send fake communications or data from the device, or add or edit code to add new capabilities or alter existing ones and erase any trace of the intrusion.

The documented attacks involving NSO Group spyware illustrate many of these privacy implications. Each of those attacks sought to compromise the personal mobile phones of the victims. Once compromised, those phones would have become total surveillance devices, photographing their environs, recording conversations and calls, accessing messages and emails, and tracking movements. By accessing this information, government authorities could have built a detailed profile of each of these individuals' lives, revealing their identity, thoughts, relationships, interests and activities.

[19] *See Reckless Exploit*, *supra*.

D. The Security Implications of Government Hacking

Hacking is an attempt to understand a system better than it understands itself, and then nudging it to do what the hacker wants. Hacking can therefore help us better understand the systems that are essential to our lives, and increasingly as they govern our lives. Hacking can also help us better understand how people use systems and how they can be manipulated to weaken or subvert the security of their own systems.

Government hacking to facilitate surveillance, on the other hand, fundamentally relies on insecurity to interfere with the right to privacy. It has the potential to undermine the security not only of the targeted device but also other unrelated systems, and even the internet as a whole. As we rely increasingly on the internet and connect more of our infrastructure to the internet this risk increases.

When the government exploits security vulnerabilities for surveillance, those vulnerabilities may also be exploited by others, particularly if the vulnerabilities (and exploits) are not reported to vendors and patched, and if the vulnerabilities nonetheless become known. The security vulnerability used by the government can not only be subsequently exploited against the targeted device itself but also against other users of the same types of device. For example, in researching the attack on Mr. Mansoor, Citizen Lab uncovered NSO Group's use of a chain of zero-day exploits (*i.e.* exploits unknown to Apple, the manufacturer of Mr. Mansoor's iPhone), which therefore placed at risk all users of iPhones. As a result of the investigation, Apple released a patch to all iPhone users and, indeed, Citizen Lab's report encouraged "[a]ll iPhone owners [to] update to the latest version of iOS (9.3.5) immediately."[20]

Government hacking powers also pose follow-on security risks: when a government deploys malware, it will not always be able to fully control its distribution. In a social engineering attack – such as the attacks using NSO Group spyware documented by Citizen Lab – links infected with malware are sent directly to targets. Such links can, for example, be forwarded onto others or posted on social media, putting at risk the devices of those individuals who unwittingly click on those links.

E. International Human Rights Analysis of Mexican Government Hacking

Because hacking entails an inherent, extensive interference with privacy and poses significant risks to the security of devices and networks, Privacy International questions whether hacking can ever be a legitimate component of state surveillance. Given the privacy and security implications of hacking, governments may never be able to demonstrate its compatibility with international human rights law, notably its necessity and proportionality as a tool for surveillance. For that reason, the U.N. Special Rapporteur on Freedom of Expression has observed:

[20] *See Million Dollar Dissident*, *supra*.

> "Offensive intrusion software such as Trojans, or mass interception capabilities, constitute such serious challenges to traditional notions of surveillance that they cannot be reconciled with existing laws on surveillance and access to private information. These are not just new methods for conducting surveillance; they are new forms of surveillance. From a human rights perspective, the use of such technologies is extremely disturbing."[21]

Below, Privacy International addresses in further detail how government hacking in Mexico specifically violates Mexico's international human rights obligations, notably Article 17 of the International Covenant on Civil and Political Rights ("ICCPR") and Article 11 of the American Convention on Human Rights ("ACHR"), which have been ratified by Mexico.

1. Mexican Government Hacking Is Not in Accordance with Law

a. The Principle of Legality

International human rights law provides that any interference with the right to privacy must be in accordance with law.[22] At the heart of the principle of legality is the important premise that placing "intrusive surveillance regimes on a statutory footing" subjects them to "public and parliamentary debate."[23] Legality is also closely tied to the concept of "arbitrary interference," the idea being that the exercise of a secret power carries the inherent risk of its arbitrary application.[24]

---

[21] Report of the U.N. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/23/40, para. 62, 17 Apr. 2013, available at http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf [hereinafter 2013 Report of the U.N. Special Rapporteur on Freedom of Expression].

[22] *See* Article 17(1), ICCPR ("No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence . . . ."); Article 11, ACHR ("2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence . . . . 3. Everyone has the right to the protection of the law against such interference . . . ."); Article 8(2) of the European Convention of Human Rights ("ECHR") ("There shall be no interference by a public authority with the exercise of [the right to respect for private and family life] except such as is in accordance with the law . . . ."); *see also* U.N. Human Rights Committee, General Comment No. 16 (Article 17 ICCPR), 8 Apr. 1988, para. 3, available at http://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/1_Global/INT_CCPR_GEC_6624_E.doc [hereinafter General Comment No. 16] (noting that "[t]he term 'unlawful' means that no interference can take place except in cases envisaged by the law" and that "[i]nterference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant"); Principle 1, International Principles on the Application of Human Rights to Communications Surveillance ("Necessary and Proportionate Principles"), available at https://necessaryandproportionate.org/principles. The Necessary and Proportionate Principles apply international human rights law to modern digital surveillance. They were drafted in 2013 by an international coalition of civil society, privacy and technology experts and have been endorsed by over 600 organizations around the world.

[23] Report of the U.N. Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, U.N. Doc. A/HRC/34/61, para. 36 (21 Feb. 2017), available at http://www.ohchr.org/Documents/Issues/Terrorism/A-HRC-34-61.pdf [hereinafter 2017 Report of the Special Rapporteur on Counter-Terrorism].

[24] Malone v. the United Kingdom, European Court of Human Rights, App. No. 8691/79, 2 Aug. 1984, para. 67 ("Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident."); *see also* General Comment No. 16, *supra*, at para. 4 (noting that "the expression 'arbitrary interference' can also

The meaning of "law" implies certain minimum qualitative requirements of accessibility and foreseeability. The U.N. Human Rights Committee has elaborated on the meaning of "law" for the purposes of Article 19 of the ICCPR, which protects the right to freedom of opinion and expression, as follows:

> "[A] norm, to be characterized as a 'law,' must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and it must be made accessible to the public. . .. Laws must provide sufficient guidance to those charged with their execution to enable them to ascertain what sorts of expression are properly restricted and what sorts are not."[25]

The Inter-American Commission on Human Rights ("IACHR") has similarly determined, in its interpretation of Article 11 of the ACHR:

> "Article 11.2 specifically prohibits 'arbitrary or abusive' interference with th[e] right [to privacy]. This provision indicates that in addition to the condition of legality, which should always be observed when a restriction is imposed on the rights of the Convention, the state has a special obligation to prevent 'arbitrary or abusive' interferences. The notion of 'arbitrary interference' refers to elements of injustice, unpredictability and unreasonableness . . . ."[26]

The requirements of accessibility and foreseeability are also reflected in the jurisprudence of the European Court of Human Rights ("ECtHR"):

> "Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a law unless it is formulated with sufficient precision to enable the citizen to regulate his conduct; he must be able—if need be with appropriate advice—to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail."[27]

The U.N. General Assembly has recognized the application of the principle of legality to the surveillance context, resolving that the "surveillance of digital communications must be

---

extend to interference provided for under the law" and that "[t]he introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims, and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances").

[25] U.N. Human Rights Committee, General Comment No. 34 (Article 19 ICCPR), 12 Sept. 2011, para. 25, available at http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf [hereinafter General Comment No. 34].

[26] Ms. X and Y v. Argentina, Inter-American Commission on Human Rights, Case 10.506, Report No. 38/96, 15 Oct. 1996.

[27] Sunday Times v. the United Kingdom, European Court of Human Rights, App. No. 6538/74, 26 Apr. 1979, para. 49.

consistent with international human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory."[28]

Both the Inter-American Court of Human Rights ("IACtHR") and the ECtHR have explicitly applied the principle of legality to the surveillance context. In *Escher et al. v. Brazil*, the IACtHR held that surveillance measures "must be based on a law that must be precise."[29] The Court further observed that the law must "indicate the corresponding clear and detailed rules, such as the circumstances in which this [surveillance] measure can be adopted, the persons authorized to request it, to order it and to carry it out, and the procedure to be followed."

Similarly, in *Weber & Saravia v. Germany*, the ECtHR elaborated on the "minimum safeguards that should be set out in statute law in order to avoid abuses of power" where the state conducts surveillance:

> "[1] the nature of the offences which may give rise to a[ ] [surveillance] order; [2] a definition of the categories of people liable to [be subject to surveillance]; [3] a limit on the duration of [surveillance]; [4] the procedure to be followed for examining, using and storing the data obtained; [5] the precautions to be taken when communicating the data to other parties; and [6] the circumstances in which [the data] may or must be erased or . . . destroyed."[30]

In 2013, the U.N. and Organization of American States Special Rapporteurs on Freedom of Expression issued a Joint Declaration on surveillance, in which they emphasized the application of the principle of legality in the surveillance context:

> "[S]tates must guarantee that the interception, collection and use of personal information, including all limitations on the right of the affected person to access this information, be clearly authorized by law in order to protect them from arbitrary or abusive interference with their private interests. The law must establish limits with regard to the nature, scope and duration of these types of measures; the reasons for ordering them; the authorities with power to authorize, execute and monitor them; and the legal mechanisms by which they may be challenged."[31]

---

[28] U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/71/199, 25 Jan. 2017, available at http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/71/199 [hereinafter U.N. General Assembly Resolution].

[29] Escher et al. v. Brazil, Inter-American Court of Human Rights, Case 12.353, 2 Mar. 2006, para. 131.

[30] Weber & Saravia v. Germany, European Court of Human Rights, App. No. 54934/00, 29 June 2006, para. 95; *see also* Malone, *supra*, at para. 67 (noting that "the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence").

[31] U.N. Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights,

b. Mexican Government Hacking Is Not in Accordance with Law

Hacking activities undertaken by the Mexican authorities, including the use of NSO Group spyware, violate the principle of legality. Mexican government hacking lacks any legal basis under the existing Mexican surveillance framework. Moreover, it is unclear whether these activities even conform to the procedures and safeguards set forth in the Mexican surveillance framework.

The Mexican surveillance framework consists of a series of constitutional and statutory sources of law. Pursuant to Article 16 of the Mexican Constitution:

> "Private communications shall not be breached. The law shall punish any action against the liberty and privacy of such communications, except when they are voluntarily given by one of the individuals involved in them. A judge shall assess the implications of such communications, provided they contain information related to the perpetration of a crime. Communications that violate confidentiality established by law shall not be admitted in any case.
>
> Only the federal judicial authority can authorize telephone tapping and interception of private communications, at the request of the appropriate federal authority or the State Public Prosecution Service. The authority that makes the request shall present in writing the legal causes for the request, describing therein the kind of interception required, the individuals subjected to interception and the term thereof. The federal judicial authority cannot authorize telephone tapping nor interception of communications in the following cases: a) when the matters involved are of electoral, fiscal, commercial, civil, labor or administrative nature, b) communications between defendant and his attorney.
>
> . . .
>
> Authorized telephone tapping and interception of communications shall be subjected to the requirements and limitations set forth in the law. The results of telephone tapping and interception of communications that do not comply with the aforesaid requirements will not be admitted as evidence."[32]

The Constitution therefore establishes certain safeguards prior to the interception of communications, including limiting such surveillance to certain federal authorities; requiring those authorities to establish the legal basis for the request and articulate the type of

---

Joint Declaration on surveillance programs and their impact on freedom of expression, 21 June 2013, para. 8, available at http://www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1.

[32] Constitution of the United Mexican States, 1917 (as amended), available at https://www.constituteproject.org/constitution/Mexico_2015.pdf?lang=en (translated into English).

interception, subjects and duration of surveillance; and mandating federal judicial authorization.

In addition to the Constitution, various Mexican federal statutes govern the surveillance activities of the government.[33] Under these statutes, three authorities are permitted to conduct the interception of communications: (1) the Public Prosecutor's Office ("PGR"), which is in charge of investigating crimes and overseeing the prosecutors' offices for each of the 32 federal entities; (2) the Federal Police; and (3) the Center for Investigations and National Security ("CISEN"). Pursuant to the Federal Criminal Procedure Code, the PGR may be granted judicial authorization to intercept communications "when there is sufficient evidence confirming the probable responsibility on the commission of a serious crime."[34] The Federal Police Law provides that the Federal Police may be granted judicial authorization to intercept communications "when there is sufficient evidence" indicating the commission of a specified list of crimes.[35] Finally, the National Security Law provides that CISEN may be granted judicial authorization to intercept communications in cases of "imminent threat to national security," which is defined as a series of categories of acts.[36]

Mexican government hacking lacks any legal basis under the existing Mexican surveillance framework, rendering it in violation of the principle of legality. The Mexican surveillance framework governs the interception of communications. As discussed above, hacking has the potential to be far more intrusive than the interception of communications and also raises unique and compelling security concerns. A framework governing the interception of communications cannot therefore address the nature of the interference with privacy posed by hacking. Thus, any interference with privacy through the use of hacking must, in and of itself, comply with the principle of legality.[37]

Moreover, it is unclear whether Mexican government hacking even conforms to the procedures and safeguards set forth in the Mexican surveillance framework. First, as discussed above, only three government authorities are permitted to intercept communications under the Mexican surveillance framework. Yet, in July 2015, the disclosure of internal documents of another surveillance company, Italy-based Hacking Team, revealed the sale of spyware to at least 14 Mexican states and government agencies, including those not authorized to conduct interception of communications pursuant to the Mexican

---

[33] For a detailed discussion of the applicable statutes, see Luis Fernando García, *State Communications Surveillance and the Protection of Fundamental Rights in Mexico*, available at https://necessaryandproportionate.org/country-reports/mexico#footnote3_1906uo2 [hereinafter *State Communications Surveillance in Mexico*] and Privacy International & R3D, *State of Privacy Mexico*, 14 Mar. 2017, available at https://www.privacyinternational.org/node/972 [hereinafter *State of Privacy Mexico*].

[34] *See State Communications Surveillance in Mexico, supra*; *State of Privacy, supra*.

[35] *See State Communications Surveillance in Mexico, supra*; *State of Privacy, supra*.

[36] *See State Communications Surveillance in Mexico, supra*; *State of Privacy, supra*.

[37] The principle of legality demands that any interferences with privacy "take place on the basis of law, which itself must comply with the provisions, aims and objectives of the [ICCPR]." General Comment No. 16, *supra*, para. 3; *see also* 2017 Report of the Special Rapporteur on Counter-Terrorism, *supra*, at para. 36 ("[P]ublicly available primary legislation is not, in itself, sufficient to ensure the compatibility of those regimes with international human rights law. Necessity, proportionality and non-discrimination must also be taken into account, along with the establishment of safeguards against arbitrariness, independent oversight and routes for redress.").

surveillance framework.[38] Like NSO Group, Hacking Team is a surveillance technology company that claims to sell its products and services exclusively to government clients. In response to the disclosures regarding Hacking Team, the IACHR Special Rapporteur for Freedom of Expression explicitly noted:

> "The surveillance software commercialized by [Hacking Team] is designed to . . . allow [ ] the gathering of information, messages, calls and emails, voice over IP and chat communication from everyday devices. This software can also remotely activate microphones and cameras . . .. [T]his Office has stated that the surveillance of communications and the interference in privacy that exceeds what is stipulated by law, which are oriented to aims that differ from those which the law permits or are carried out clandestinely, must be harshly punished. Such illegitimate interference includes actions taken for political reasons against journalists and independent media."[39]

Given the similarities between NSO Group and Hacking Team as well as between their spyware products, it seems reasonable to question whether Mexican government authorities not authorized to conduct surveillance activities were behind the purchase and use of the NSO Group spyware at issue in the recent attacks against journalists, human rights defenders and activists.

In addition, the Mexican surveillance framework requires that the interception of communications be authorized by a federal judicial authority. Mexican civil society has expressed scepticism that the earlier attacks against Mexican "soda tax" advocates were judicially authorized.[40] Former Mexican intelligence officials have similarly expressed doubts that Mexican government authorities sought judicial authorization for the most recently reported attacks against journalists and human rights defenders.[41] (And in any event, the Mexican surveillance framework provides no legal basis for hacking such that it could be judicially authorized). Such scepticism is warranted given the profiles of the victims of these attacks. The Mexican surveillance framework limits the interception of communications to

---

[38] *See* Mattathias Schwartz, *Cyberware for Sale*, N.Y. Times, 4 Jan. 2017, available at https://www.nytimes.com/2017/01/04/magazine/cyberwar-for-sale.html; Arturo Ángel, *Sedena negoció compra de software a Hacking Team en 2015 para espiar a 600 personas*, Animal Político, 21 July 2015, available at http://www.animalpolitico.com/2015/07/sedena-negocio-compra-de-software-a-hacking-team-en-2015-para-espiar-a-600-personas/; Arturo Ángel, *México, el principal cliente de una empresa que vende software para espiar*, Animal Político, 7 July 2015, available at http://www.animalpolitico.com/2015/07/empresa-de-hackers-exhibida-por-venta-de-software-espia-a-paises-represores-y-mexico-resulta-su-principal-cliente/. These disclosures also revealed that Mexico was Hacking Team's largest client.

[39] Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Concern Over the Acquisition and Implementation of Surveillance Programs by States of the Hemisphere, Press Release R80/15, 21 July 2015.

[40] *See Spyware's Odd Targets*, *supra.*

[41] *See Reckless Exploit*, *supra* ("'Mexican security agencies wouldn't ask for a court order, because they know they wouldn't get one,' said Eduardo Guerrero, a former analyst at the Center for Investigation and National Security, Mexico's intelligence agency and one of the government agencies that use the Pegasus spyware. 'I mean, how could a judge authorize surveillance of someone dedicated to the protection of human rights?' 'There, of course, is no basis for that intervention, but that is besides the point,' he added. 'No one in Mexico ever asks for permission to do so.'").

circumstances involving crime and national security. None of the victims appear to have been targeted for such purposes.

2. Mexican Government Hacking Is Neither Necessary Nor Proportionate

a. Necessity and Proportionality

International human rights law requires that any interference with the right to privacy must not only be in accordance with law but must also be necessary and proportionate.[42] The principle of necessity "implies that restrictions must not simply be useful, reasonable or desirable to achieve a legitimate government object," but rather, that "a State must demonstrate in 'specific and individualized fashion the precise nature of the threat' that it seeks to address, and a 'direct and immediate connection between the expression and the threat.'"[43] This concept of necessity is also sometimes expressed as requiring that any interference with the right to privacy be "necessary to achieve a legitimate aim."[44]

The IACHR Special Rapporteur for Freedom of Expression has applied the principle of necessity to the surveillance context, noting that "in order for an online communications surveillance program to be appropriate, States must demonstrate that the limitations to the rights to privacy and freedom of expression arising from those programs are strictly

---

[42] *See* U.N. Human Rights Committee, Toonen v. Australia, Comm. No. 488/1992, U.N. Doc. CCPR/C/50/D/488/1992 (31 Mar. 1994), para. 8.3 ("[A]ny interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case."); Office of the U.N. High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/27/37 (30 June 2014), para. 23, available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G14/088/54/PDF/G1408854.pdf?OpenElement [hereinafter 2014 OHCHR Report] ("These authoritative sources [HRC General Comments 16, 27, 29, 31, and 34 and the Siracusa Principles] point to the overarching principles of legality, necessity and proportionality . . . ."); U.N. Human Rights Council Resolution on the Right to Privacy in the Digital Age U.N. Doc. A/HRC/34/7, 23 Mar. 2017, para. 2 available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/086/31/PDF/G1708631.pdf?OpenElement ("*Recall[ing]* that States should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity and proportionality").

[43] Brief of Amici Curiae, U.N. Human Rights Experts in Support of Plaintiff-Appellant and Reversal, John Doe (Kidane) v. The Federal Democratic Republic of Ethiopia, D.C. Ct. App., No. 16-7081, p. 14 (1 Nov. 2016) , available at https://www.eff.org/files/2016/11/01/11.1.16_united_nations_human_rights_experts_amicus_brief.pdf (citing General Comment No. 34, *supra*, at 35) [hereinafter Brief of U.N. Human Rights Experts]. The U.N. human rights experts authoring the brief were the U.N. Special Rapporteurs on Freedom of Expression, Freedom of Peaceful Assembly, and the Situation of Human Rights Defenders.

[44] Article 30 ACHR provides that restrictions of the rights recognized by the Convention "may not be applied except in accordance with laws enacted for reasons of general interest and in accordance with the purpose for which such restrictions have been established." Article 8 ECHR is somewhat more specific, providing that "[t]here shall be no interference by a public authority with the exercise" of the right to privacy "except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." *See also* 2014 OHCHR Report, *supra*, para. 23 ("The limitation must be necessary for reaching a legitimate aim . . . . The onus is on the authorities seeking to limit the right to show that the limitation is connected to a legitimate aim."); Principle 2, Necessity and Proportionate Principles ("Laws should only permit Communications Surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society.").

necessary in a democratic society to accomplish the objectives they pursue."[45] In addition, the Special Rapporteur observed that, "it is insufficient for the measure to be 'useful,' 'reasonable,' or 'opportune.'" Rather, the State must clearly establish "the true and compelling need to impose the limitation."

The ECtHR has also had occasion to apply the principle of necessity to interferences with Article 8 in the surveillance context. In *Szabó & Vissy v. Hungary*, the ECtHR indicated that given "the potential of cutting-edge surveillance technologies to invade citizens' privacy," the "legitimate aim" requirement had to be interpreted strictly as follows:

> "A measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding the democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation. In the Court's view, any measure of secret surveillance which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal. The Court notes that both the Court of Justice of the European Union and the United Nations Special Rapporteur require secret surveillance measures to answer to strict necessity – an approach it considers convenient to endorse."[46]

The principle of proportionality requires that the interference with privacy be both "in proportion to the aim and the least intrusive option available."[47] The U.N. Special Rapporteur for Counter-Terrorism has provided additional guidance to States on demonstrating proportionality in the surveillance context. He has submitted that "proportionality involves balancing the extent of the intrusion into Internet privacy rights against the specific benefit accruing to investigations undertaken by a public authority in the public interest."[48] He has also indicated that "[i]n the context of covert surveillance . . . [t]he proportionality of any interference with the right to privacy should . . . be judged on the particular circumstances of the individual case." He emphasized, however, that "in no case may the restrictions be

---

[45] Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, *Freedom of Expression and the Internet*, 31 Dec. 2013, paras. 159-60, available at http://www.oas.org/en/iachr/expression/docs/reports/2014_04_08_internet_eng%20_web.pdf [hereinafter 2013 Report of the IACHR Special Rapporteur].

[46] Szabó & Vissy v. Hungary, App. No. 37138/14, 12 Jan. 2016, para. 73.

[47] 2014 OHCHR Report, *supra*, at para. 23; *see also* U.N. Human Rights Committee, Toonen v. Australia, *supra*, at para. 8.3.; Report of the U.N. Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, A/HRC/13/37, 28 Dec. 2009, para. 49, available at http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf ("[P]rotections [of the right to privacy] require States to have exhausted less-intrusive techniques before resorting to others. . . . States must incorporate this principle into existing and future policies as they present how their policies are necessary, and in turn proportionate."); Brief of U.N. Human Rights Experts, *supra*, pp. 14-15 (stating that proportionality requires that "the restrictions are . . . the least intrusive amongst those which might achieve their protective function . . . [and] proportionate to the interest to be protected"); Principle 5, Necessity and Proportionate Principles.

[48] Report of the U.N. Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, U.N. Doc. A/69/397, para. 51 (23 Sept. 2014).

applied or invoked in a manner that would impair the essence of a Covenant right." The Office of the U.N. High Commissioner for Human Rights has similarly observed that "any limitation to the right to privacy must not render the essence of the right meaningless and must be consistent with other human rights."[49]

The IACHR Special Rapporteur for Freedom of Expression has also weighed in on the proportionality analysis in the surveillance context, indicating that "in order to define if a measure is proportioned, its impact on the capacity of the Internet to guarantee and promote freedom of expression should be evaluated."[50] The Special Rapporteur also urged that "[g]iven the importance of the exercise of these rights in a democratic system, the law must authorize access to personal data and communications only under the most exceptional circumstances defined in the law." The Special Rapporteur observed:

> "When fairly open-ended grounds such as national security are invoked as the reason to monitor personal data and correspondence . . . [t]heir application should be authorized solely when there is a definite risk to the protected interests, and when that harm is greater than society's general interest in maintaining the rights to privacy and the free expression of thought and the circulation of information."

b. Mexican Government Hacking Is Neither Necessary Nor Proportionate

Reported hacking activities undertaken by the Mexican authorities are neither necessary nor proportionate. The documented attacks against journalists, human rights defenders and activists, are not necessary because they are not in pursuit of a legitimate aim.

As a threshold matter, Mexican authorities have failed to assert any public justification for its surveillance of these individuals. In any event, none of these individuals would appear to be legitimate targets pursuant to the Mexican surveillance framework, which limits the interception of communications to circumstances involving crime and national security. Indeed, Mexican authorities appear to have targeted these victims for reasons prohibited under international human rights law. Under international human rights law, "'the muzzling of any advocacy of multi-party democracy, democratic tenets and human rights' is never a legitimate objective; in fact it undermines public engagement and debate in a matter that runs counter to the letter of Article 19 [ICCPR] and the object and purposes of the Covenant."[51] Thus, Mexican authorities cannot justify hacking activities as necessary in pursuit of a legitimate aim where they target journalists, human rights defenders and activists for their public advocacy and human rights work.

---

[49] 2014 OHCHR Report, *supra*, para. 23; *see also* Zakharov v. Russia, European Court of Human Rights, App. No. 47143/06, 4 Dec. 2015, para. 232 (observing that there existed "the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it").
[50] 2013 Report of the IACHR Special Rapporteur, *supra*, at paras. 161-62.
[51] Brief of U.N. Human Rights Experts, *supra*, p. 15 (citing General Comment No. 34, *supra*, at para. 23).

Because Mexican authorities cannot justify their hacking activities as necessary, an analysis of their proportionality is moot. The proportionality assessment balances the scope of the interference with privacy against the legitimate aim sought by the state. Thus, a prerequisite to the proportionality assessment is a legitimate aim, which is lacking here.

Nevertheless, Privacy International takes this opportunity to emphasize that the extensive interference with privacy posed by hacking – as well as the risks that it poses to the security of our devices and networks – suggests that this activity may be inherently disproportionate. Should Mexican authorities continue to insist on hacking for surveillance purposes, it bears the difficult burden of demonstrating how these activities can be reconciled with international human rights law and, in particular, the requirement of proportionality.

3. The Existing Mexican Surveillance Framework Lacks Appropriate Safeguards

Privacy International also takes this opportunity to note with concern that Mexico's current surveillance framework – even as it applies to the interception of communications – lacks certain safeguards critical to ensuring its compliance with international human rights law.[52] While it is beyond the scope of this letter to elaborate on each of these safeguards, they include, *inter alia*, notification to targets of surveillance,[53] effective oversight,[54] and transparency requirements.[55]

---

[52] General Comment No. 16, *supra*, at para. 10; *see also* Uzun v. Germany, European Court of Human Rights, App. No. 35623/05, 2 Sept. 2010, para. 63 ("[I]n the context of secret measures of surveillance by public authorities, because of the lack of public scrutiny and the risk of misuse of power, compatibility with the rule of law requires that domestic law provides adequate protection against arbitrary interference with Article 8 rights. The Court must be satisfied that there exist adequate and effective guarantees against abuse. This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law.").

[53] *See* General Comment No. 16, *supra*, at para. 10 ("In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files."); U.N. Human Rights Committee, Concluding Observations on the Third Periodic Report of the Former Yugoslav Republic of Macedonia, U.N. Doc. CCPR/C/MKD/CO/3, 17 Aug. 2015, para. 23 ("[The State Party should] ensure that persons who are unlawfully monitored are systematically informed thereof and have access to adequate remedies."); 2013 Report of the U.N. Special Rapporteur on Freedom of Expression, *supra*, at para. 82 ("Individuals should have a legal right to be notified that they have been subjected to communications surveillance or that their communications data has been accessed by the State. Recognizing that advance or concurrent notification might jeopardize the effectiveness of the surveillance, individuals should nevertheless be notified once surveillance has been completed . . . .").

[54] *See* U.N. General Assembly Resolution, *supra*, para. 4 ("*Calls upon all States* . . . (d) To establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data . . . ."); U.N. Human Rights Committee, Concluding Observations on the Sixth Periodic Report of Canada, U.N. Doc CCPR/C/CAN/CO/6, 13 Aug. 2015, para. 10 ("The Committee is also concerned about the lack of adequate and effective oversight mechanisms to review activities of security and intelligence agencies and the lack of resources and power of existing mechanisms to monitor such activities . . . . The State Party should . . . (d) Establish oversight mechanisms over security and intelligence agencies that are effective and adequate and

The current Mexican surveillance framework lacks each of these important safeguards. It does not require Mexican authorities to notify subjects targeted by surveillance. It does not provide for independent oversight mechanisms to provide ex post review of surveillance. Nor does it establish transparency reporting requirements. Privacy International therefore urges Mexico to establish these safeguards so as to render its current surveillance framework compatible with international human rights law.

F. Conclusion

For the reasons set forth above, Mexican government hacking, including the use of NSO Group spyware, raises grave human rights concerns and calls into question whether Mexico is meeting its obligations under international human rights law. Privacy International therefore urges Mexican authorities to immediately cease all hacking activities. We further support the calls by the victims for an independent inquiry and call on the Attorney General's Office to conduct a prompt, thorough and credible investigation of the criminal complaint.

In addition, Privacy International and R3D make the following further recommendations.

To the President of the United Mexican States to:

- Make public what hacking activities Mexican authorities have undertaken to date and by which authorities, including avowing the reported use of NSO Group spyware against journalists, human rights defenders and activists;
- Clarify the Mexican government's understanding of the legal basis for its hacking activities and what rules and safeguards, if any, regulate its hacking activities;
- Confirm what types of hacking tools, including malware, are employed by Mexican authorities and how the acquisition and use of these technologies is regulated and monitored.

To the Attorney General's Office, the General Congress of the United Mexican States, the National Human Rights Commission, the Mechanism to Protect Human Rights Defenders and Journalists, and the National Institute for Transparency, Access to Information and Personal Data Protection to:

---

provide them appropriate powers as well as sufficient resources to carry out their mandate . . . ."); 2013 Report of the U.N. Special Rapporteur on Freedom of Expression, *supra*, at para. 93 ("States should establish independent oversight mechanisms capable to ensure transparency and accountability of State surveillance of communications.").

[55] *See* 2013 Report of the U.N. Special Rapporteur on Freedom of Expression, *supra*, at para. 91 ("States should be completely transparent about the use and scope of communications surveillance techniques and powers. They should publish, at minimum, aggregate information on the number of requests approved and rejected, a disaggregation of the requests by service provider and by investigation and purpose."); 2013 Report of the IACHR Special Rapporteur, *supra*, at paras. 168 ("States should disclose general information on the number of requests for interception and surveillance that have been approved and rejected, and should include as much information as possible, such as – for example – a breakdown of requests by service provider, type of investigation, time period covered by the investigations, etc.").

- Conduct prompt, thorough and independent investigations into:
    - The nature and scope of government hacking activities, including whether such activities are compliant with international and domestic law;
    - The reported use of NSO Group spyware against journalists, human rights defenders and activists, with a view to bringing to justice the perpetrators and providing redress to the victims of these abuses;
    - The types of hacking tools, including malware, employed by Mexican authorities and whether their acquisition and use are compliant with international and domestic law.
- Make publicly available any findings related to the above investigations.

To all Mexican authorities that are conducting or have conducted hacking activities to:

- Notify all targets of their hacking activities to date, indicating the purported legal basis and relevant rules, if any, governing such activities;
- Destroy all material obtained through their hacking activities;
- Provide all targets of their hacking activities with an avenue for redress.