IN THE EUROPEAN COURT OF HUMAN RIGHTS **APP. NO. 24960/15**

BETWEEN:

10 HUMAN RIGHTS ORGANISATIONS

Applicants

-v-

UNITED KINGDOM

Respondent Government

FACTUAL APPENDIX TO APPLICANTS' REPLY TO OBSERVATIONS OF THE GOVERNMENT OF THE UNITED KINGDOM

1. The Applicants provide this factual appendix to address several additional facts related to the United Kingdom's bulk interception programme pursuant to section 8(4) of the Regulation of Powers Act ("RIPA") (the "s8(4) Regime") and the United States of America's bulk surveillance programmes pursuant to Executive Order 12333 and section 702 of the Foreign Intelligence Surveillance Act ("FISA").

2. The first set of facts describe the GCHQ programmes KARMA POLICE, Black Hole and MUTANT BROTH, which shed light on the ways in which the UK Government uses bulk interception, particularly to create detailed profiles of individuals around the world. The Government creates these profiles without any regard to whether it possesses reasonable suspicion that such individuals are committing or have committed a criminal offence or are a threat to national security.

3. The second set of facts provide further detail on the bulk nature of US surveillance programmes:

a. First, the Applicants describe the NSA programmes MYSTIC, DISHFIRE, CO-TRAVELLER, MUSCULAR and XKEYSCORE, which appear to operate pursuant to Executive Order 12333. The Applicants presented evidence of these programmes to the Investigatory Powers Tribunal ("IPT"), gathered from public reporting of leaked NSA and GCHQ documents.

b. Second, the Applicants provide information regarding additional bulk surveillance programmes that have surfaced in the public domain – WINDSTOP, INCENSER, RAMPART-A and MARINA – which also appear to operate under Executive Order 12333 and further illuminate the "bulk" nature of US surveillance under this framework.

c. Finally, the Applicants discuss in detail PRISM and Upstream, two programmes operating under section 702 of FISA. The Government describes both programmes as targeted and the Applicants elaborate on why that characterisation is flawed.

I. UK Bulk Interception: KARMA POLICE, Black Hole and MUTANT BROTH

4. On 25 September 2015, *The Intercept* published a selection of previously unreleased documents obtained from Edward Snowden.[1] These documents detailed three surveillance programmes operated by GCHQ, codenamed KARMA POLICE, Black Hole and MUTANT BROTH, which reveal what happens to communications data intercepted in bulk by the UK Government.

A. KARMA POLICE

[1] Ryan Gallagher, *Profiled: From Radio to Porn, British Spies Track Web Users' Online Identities*, THE INTERCEPT, 25 Sept. 2015, https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities/ ("*British Spies Track Web Users' Online Identities*").

5. According to the minutes of a GCHQ steering committee dated 29 February 2008, "*KARMA POLICE aims to correlate every user visible to passive [signals intelligence] with every website they visit, hence providing either (a) a web browsing profile for every visible user on the internet, or (b) a user profile for every visible website on the internet.*"[2]

6. *The Intercept* revealed that, over a 3-month period in 2009, KARMA POLICE gathered "*nearly 7 million metadata records*" in order "*to observe the listening habits of more than 200,000 people across 185 countries, including the US, the UK, Ireland, Canada, Mexico, Spain, the Netherlands, France and Germany.*"[3] As part of this operation, GCHQ analysts, for example, "*zeroed in on any stations found broadcasting recitations from the Quran*" and then "*used KARMA POLICE to find out more about these stations' listeners, identifying them as users on Skype, Yahoo, and Facebook.*"[4]

B. Black Hole

7. Black Hole is a repository, which contains internet data "*collected by GCHQ as part of bulk 'unselected' surveillance, meaning it is not focused on particular 'selected' targets*" but rather, stores "*raw logs of intercepted material before it has been subject to analysis.*"[5] A 2009 GCHQ PowerPoint presentation reveals that, between August 2007 and March 2009, Black Hole "*was used to store more than 1.1 trillion 'events' – a term the agency uses to refer to metadata records – with about 10 billion new entries added every day.*"[6] It also indicated that "*the largest slice of data*

[2] *Pull Through Steering Group Minutes*, dated 29 Feb. 2008, published in THE INTERCEPT, 25 Sept. 2015, https://theintercept.com/document/2015/09/25/pull-steering-group-minutes/.
[3] *British Spies Track Web Users' Online Identities.*
[4] *British Spies Track Web Users' Online Identities.*
[5] *British Spies Track Web Users' Online Identities.*
[6] *QFD BLACKHOLE Technology Behind INOC*, Mar. 2009, published in in THE INTERCEPT, 25 Sept. 2015, https://theintercept.com/document/2015/09/25/qfd-blackhole-technology-behind-inoc/ ("*QFD BLACKHOLE Technology*").

Black Hole held – 41 percent – was about people's internet browsing histories."[7] The remainder consisted of "*a combination of email and instant messenger records, details about search engine queries, information about social media activity, logs related to hacking operations, and data on people's use of tools to browse the internet anonymously.*"[8] A 2011 GCHQ PowerPoint presentation describes GCHQ's development of "'*unprecedented' techniques to perform…'population-scale' data mining, monitoring all communications across entire countries in an effort to detect patterns or behaviours deemed suspicious.*"[9]

8. A 2012 GCHQ PowerPoint presentation reveals that GCHQ's interception capabilities had increased to the point where it was intercepting "*approximately 50 billion events per day from 250+ x10G bearers*" but that it was working to double capacity to 100 billion events per day.[10] The presentation also indicates that GCHQ was sharing this material with "*foreign partners*" through "*[w]eb user interfaces…on GCHQ servers but accessible from the partner site*" and through "*[b]rokering services*", permitting "*[s]ustained access for interactive query of GCHQ data integrated into partner tools.*"[11]

C. MUTANT BROTH

[7] *British Spies Track Web Users' Online Identities*; *QFD BLACKHOLE Technology*.

[8] *British Spies Track Web Users' Online Identities*; *QFD BLACKHOLE Technology*.

[9] *British Spies Track Web Users' Online Identities*; *Cloud Developers Exchange July 2011*, published in THE INTERCEPT, 25 Sept. 2015, https://theintercept.com/document/2015/09/25/cloud-developers-exchange-july-2011/.

[10] *GCHQ Analytic Cloud Challenges*, published in THE INTERCEPT, 25 Sept. 2015, https://theintercept.com/document/2015/09/25/gchq-analytic-cloud-challenges/ ("*GCHQ Analytic Cloud Challenges*").

[11] *GCHQ Analytic Cloud Challenges*.

9. MUTANT BROTH is a GCHQ system, which is "*used to sift through data contained in the Black Hole repository about vast amounts of tiny intercepted files known as cookies*."[12] Cookies are stored on computers to identify and sometimes track people browsing the internet. For that reason, GCHQ refers to cookies as "*target detection identifiers*" or "*presence events*" because "*they help it monitor people's internet use and uncover online identities*".[13] A 2009 GCHQ PowerPoint presentation reveals that GCHQ has targeted popular websites, including Facebook, YouTube, Amazon and BBC in order to amass cookies.[14] The presentation further indicates that in a six-month period between December 2008 and June 2008, over 18 billion records were accessible through MUTANT BROTH.[15]

II. US Bulk Surveillance

A. Executive Order 12333

1. MYSTIC, DISHFIRE, CO-TRAVELLER, OPTIC NERVE, MUSCULAR and XKEYSCORE

10. The Applicants presented evidence of the following bulk surveillance programmes to the IPT:[16]

[12] *British Spies Track Web Users' Online Identities.*
[13] *British Spies Track Web Users' Online Identities.*
[14] *TDI Introduction*, published in THE INTERCEPT, 25 Sept. 2015, https://theintercept.com/document/2015/09/25/tdi-introduction/ ("*TDI Introduction*").
[15] *TDI Introduction.*
[16] Witness Statement of Eric King, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs et al.*, IPT/13/92/CH, 8 June 2014, paras 106-113, 134-141 (lodged with the Court in the List of Accompanying Documents in the original Application). At the time that the Applicants issued proceedings before the IPT, they understood these programmes as forming part of the FISA section 702 regime that governs the PRISM and Upstream programmes. This lack of clarity was a result of the fact that information as to the scope and nature of these programmes was and continues to be limited primarily to public domain information. Where it is unclear whether a programme is still active, the Applicants have described it in the present tense.

a. MYSTIC is a US National Security Agency ("NSA") programme that intercepts, extracts and stores the communications data of all mobile phone calls made to, from or within targeted countries, including Mexico, the Philippines and Kenya.[17] It has been implemented in countries with a combined population of more than 250 million.[18] SOMALGET is an NSA programme that intercepts, extracts and stores all of the content of every mobile phone call made to, from, and within the Bahamas and Afghanistan.[19]

b. DISHFIRE is an NSA programme that intercepts, extracts and stores the content and communications data of 194 million text messages per day.[20] According to documents obtained from GCHQ, the NSA collects "*pretty much everything it can*".[21] The programme does not involve "*merely storing the communications of existing surveillance targets*".[22] DISHFIRE has reportedly been used each day, on average, to identify 1.6 million border crossings, 110,000 names from electronic business cards and 800,000 financial transactions by text-to-text payments or linking credit cards to phone users.[23]

[17] Ryan Devereaux, Glenn Greenwald & Laura Poitras, *Data Pirates of the Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas*, THE INTERCEPT, 19 May 2014, https://theintercept.com/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/ (cited in King Witness Statement, para 111-12) ("*Data Pirates of the Caribbean*"); Barton Gellman and Ashkan Soltani, *NSA surveillance program reaches 'into the past' to retrieve, replay phone calls*, THE WASHINGTON POST, 18 Mar. 2014, https://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html (cited in King Witness Statement, para 111).

[18] *Data Pirates of the Caribbean.*

[19] *Data Pirates of the Caribbean.* THE INTERCEPT did not identify Afghanistan in its report; this information was later revealed by Wikileaks. *WikiLeaks statement on the mass recording of Afghan telephone calls by the NSA*, WIKILEAKS, 23 May 2013, https://wikileaks.org/WikiLeaks-statement-on-the-mass.html.

[20] James Ball, *NSA collects millions of text messages daily in 'untargeted' global sweep*, THE GUARDIAN, 16 Jan. 2014, https://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep (cited in King Witness Statement, para 106) ("*NSA collects millions of text messages daily*").

[21] *NSA collects millions of text messages daily.*

[22] *NSA collects millions of text messages daily.*

[23] *NSA collects millions of text messages daily.*

c. CO-TRAVELLER is an NSA programme that intercepts, extracts and stores "*nearly 5 billion records a day on the whereabouts of cellphones around the world*".[24] An anonymous NSA employee explained that the NSA was "'*getting vast volumes' of location data…by tapping into the cables that connect mobile networks globally and that serve U.S. cellphones as well as foreign ones*."[25]

d. MUSCULAR was a programme by which the NSA (together with GCHQ) intercepted and extracted data directly as it transited to and from Google and Yahoo's private data centres, which are located around the world.[26] According to a leaked 2013 NSA document, "*the NSA…sends millions of records every day from internal Yahoo and Google networks to data warehouses at the agency's headquarters at Fort Meade, Md.*"[27] In one 30-day period, the document stated, "*field collectors had processed and sent back 181,820,466 new records – including 'metadata'…as well as content such as text, audio and video*."[28]

e. XKEYSCORE is an NSA "*processing and query system*", fed by "*a constant flow of Internet traffic from fiber optic cables that make up the backbone of the world's communication network, among other*

[24] Barton Gellman & Ashkan Soltani, *NSA tracking cellphone locations worldwide, Snowden documents show*, THE WASHINGTON POST, 4 Dec. 2013, https://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html (cited in King Witness Statement, para 107) ("*NSA tracking cellphone locations worldwide*").

[25] *NSA tracking cellphone locations worldwide.*

[26] Barton Gellman & Ashkan Soltani, *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say*, THE WASHINGTON POST, 30 Oct. 2013, https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html (cited in King Witness Statement, paras 134-136) ("*NSA infiltrates links to Yahoo, Google*").

[27] *NSA infiltrates links to Yahoo, Google.*

[28] *NSA infiltrates links to Yahoo, Google.*

sources".[29] As of 2008, XKEYSCORE "*boasted approximately 150 field sites*" including in the US and UK, "*consisting of over 700 servers*".[30] Those servers store "'*full-take data' at the collection sites – meaning that they captured all of the traffic collected*".[31] XKEYSCORE then permits analysts "*to query the system to show the activities of people based on their location, nationality and websites visited.*"[32]

11. The US Government has publicly acknowledged a number of the programmes described above. In December 2013, speaking anonymously, but with permission from the NSA, an NSA employee explained that through CO-TRAVELLER the NSA was able to obtain "*vast volumes*" of location data by tapping cables that connect mobile networks globally.[33] In January 2014, the NSA publicly acknowledged the existence of DISHFIRE in response to reporting about the programme.[34] The US Director of National Intelligence, James Clapper, also appears to have alluded publicly to the existence of MYSTIC and SOMALGET in 2015.[35]

2. WINDSTOP, INCENSER, RAMPART-A and MARINA

12. Apart from evidence presented by Applicants to the IPT, additional information regarding bulk surveillance programmes appearing to operate

[29] Morgan Marquis-Boire, Glenn Greenwald & Micah Lee, *XKEYSCORE: NSA's Google for the World's Private Communications*, THE INTERCEPT, 1 July 2013, https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/ (cited in King Witness Statement, para 139) ("*XKEYSCORE: NSA's Google*"); Glenn Greenwald, *XKeyscore: NSA tool collects 'nearly everything a user does on the internet*', THE GUARDIAN, 31 July 2013, https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data (cited in King Witness Statement, para 140).

[30] *XKEYSCORE: NSA's Google*

[31] *XKEYSCORE: NSA's Google.*

[32] *XKEYSCORE: NSA's Google.*

[33] *NSA tracking cellphone locations worldwide.*

[34] *NSA collects millions of text messages daily* ("*[T]he NSA spokeswoman said:…'Dishfire is a system that processes and stores lawfully collected SMS data.*").

[35] Ellen Nakashima, *Top spy bemoans loss of key information-gathering program*, THE WASHINGTON POST, 9 Sept. 2015, https://www.washingtonpost.com/world/national-security/top-spy-bemoans-loss-of-key-intelligence-program/2015/09/09/a214bda4-5717-11e5-abe9-27d53f250b11_story.html.

under the auspices of Executive Order 12333 has also been publicly reported:

a. WINDSTOP is an umbrella programme for bulk interception, which the NSA operates in partnership with the agencies of the Five Eyes.[36] The programme aims to "*develop a well-integrated, over-arching architecture to utilize unprecedented access to communications into and out of Europe and the Middle East.*"[37] One of the WINDSTOP programmes is MUSCULAR, which the Applicants identified to the IPT, involves intercepting "*Google and Yahoo internal data flows*".[38] Another WINDSTOP programme is INCENSER, a "*high-volume cable tapping programme*" operated by the NSA (together with GCHQ).[39] Between 12 December 2012 and 8 January 2013, WINDSTOP collected more than 14 billion metadata records.[40] XKEYSCORE, another programme the Applicants identified to the IPT processes and searches data collected under WINDSTOP.[41]

b. INCENSER is the "*NSA's fourth largest cable tapping programme" with "just over 14 billion pieces of internet data a month.*"[42] The interception takes place at a location in Cornwall codenamed

[36] *One month, hundreds of millions of records collected*, THE WASHINGTON POST, www.washingtonpost.com/apps/g/page/world/one-month-hundreds-of-millions-of-records-collected/554/ ("*One month, hundreds of millions of records*").
[37] "*(U) Special Source Access, (U) Foreign Partner Access*" (Snowden document), published by Statewatch, http://www.statewatch.org/news/2014/jun/usa-nsa-foreignpartneraccessbudgetfy2013-redacted.pdf ("*Special Source Access*"). Other WINDSTOP related Snowden documents have been published on the websites of the American Civil Liberties Union, https://www.aclu.org/files/assets/2013.10.30%20NSA%20Special%20Operations%20Weekly%20Excerpt.pdf, and the Electronic Frontier Foundation, https://www.eff.org/files/2014/04/09/20131104-wapo-windstop.pdf.
[38] *One month, hundreds of millions of records.*
[39] *One month, hundreds of millions of records.*
[40] *WINDSTOP – Last 30 Days* (Snowden document), published by Electronic Frontier Foundation, https://www.eff.org/files/2014/04/09/20131104-wapo-windstop.pdf ("*WINDSTOP – Last 30 Days*").
[41] *One month, hundreds of millions of records; WINDSTOP – Last 30 Days.*
[42] *INCENSER, or how NSA and GCHQ are tapping internet cables*, Eletrospaces.net, 29 Nov. 2014, http://electrospaces.blogspot.co.uk/2014/11/incenser-or-how-nsa-and-gchq-are.html ("*INCENSER, NSA and GCHQ*").

NIGELLA with the help of a British telecommunications company.[43] INCENSER intercepts information travelling over FLAG ATLANTIC 1 (connecting the east coast of North America to the UK and France) and FLAG EUROPE ASIA (connecting the UK to Japan through the Mediterranean and including landing points in Egypt, the Saudi Peninsula, India, Malaysia, Thailand, Hong Kong, China, Taiwan, and South Korea).[44]

c. RAMPART-A is an NSA programme launched in 1992 with the aim of gaining "*access to high capacity international fiber-optic cables that transit at major congestion points around the world*".[45] The NSA operates RAMPART-A in conjunction with foreign partners, who "*provide access to cables and host US equipment*", while the US "*provides equipment for transport, processing, and analysis" of intercepted information*.[46] The partnerships also involve "*[s]hared tasking & collection*".[47] RAMPART-A has "*access to over 3 Terabits per second of data streaming world-wide and encompasses all communication technologies such as voice, fax, telex, modem, e-mail internet chat, Virtual Private Network (VPN), Voice over IP (VoIP), and voice call records*."[48]

d. MARINA is the NSA's communications data depository.[49] According to an introductory guide for NSA field agents, disclosed by Snowden, "*[a]ny computer metadata picked up by NSA collection systems is*

[43] *INCENSER, NSA and GCHQ.*

[44] *INCENSER, NSA and GCHQ.*

[45] *RAMPART-A: Project Overview* (Snowden document), 1 Oct. 2010, published by Electronic Frontier Foundation, www.eff.org/files/2014/06/23/rampart-a_overview.pdf ("*RAMPART-A: Project Overview*").

[46] *RAMPART-A: Project Overview.*

[47] *RAMPART-A: Project Overview.*

[48] *Special Source Access.*

[49] James Ball, *NSA stores metadata of millions of web users for up to a year, secret files show*, THE GUARDIAN, 30 Sep. 2013, www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents ("*NSA stores metadata of millions*").

routed to the Marina database".[50] The guide explains that, "*[o]f the more distinguishing features, Marina has the ability to look back on the last 365 days' worth of…metadata seen by the Sigint collection system, regardless whether or not it was tasked for collection.*"[51] MARINA aggregates NSA metadata "*from an array of sources, some targeted*", others based on bulk surveillance, including the NSA's fibre-optic tapping programs.[52]

B. Section 702 of FISA: Upstream and PRISM

13. The UK Government describes PRISM and Upstream as "targeted" rather than "bulk" programmes and states that they require the NSA to identify a specific person whose communications or communications data are to be obtained (Observations, §1.6(2)).

14. Upstream, much like the s8(4) Regime, involves intercepting and extracting information traveling along the "*the telecommunications backbone over which communications transit*", including both telephone and internet communications.[53] In describing the s8(4) Regime, the UK Government

[50] *NSA stores metadata of millions.*

[51] *NSA stores metadata of millions.*

[52] *NSA stores metadata of millions.*

[53] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2014) p 35, *available at* https://www.pclob.gov/library/702-Report.pdf ("PCLOB, s702 Report"). A factual point of contention concerns whether the NSA or telecommunications companies are conducting the interception, extraction and/or filtering. A report from the NSA's inspector general, declassified in February 2016, suggests that the NSA provides selectors to the companies, which then apply them and turn over captured communications. In particular, the report states that "[f]or upstream Internet collection and telephony collection, the communication service providers who control the telecommunications infrastructure over which the communications travel are legally compelled to make available to NSA communications related to tasked selectors." OFFICE OF THE INSPECTOR GENERAL, NSA, IMPLEMENTATION OF §215 OF THE USA PATRIOT ACT AND §702 OF THE FISA AMENDMENTS ACT OF 2008 (2015) p 94, *available at* https://www.documentcloud.org/documents/2712306-Savage-NYT-FOIA-IG-Reports-702-2.html. In the past, however, the US Government has used ambiguous language, leaving unclear whether the NSA or the companies themselves were conducting these steps. Charlie Savage, *N.S.A. Gets Less Web Data Than Believed, Report Suggests*, N.Y. TIMES, 16 Feb. 2016, http://www.nytimes.com/2016/02/17/us/report-says-networks-give-nsa-less-data-than-long-suspected.html (citing PCLOB, s702 Report) and Memorandum in Support of Defendants' Motion

repeatedly indicates that "*it intercepts communications in 'bulk' – that is, at the level of communications cables*". (Observations, §1.21). The Government explains the "*technical reasons*" for bulk interception:

> "*[C]ommunications sent over the internet are broken down into small pieces, known as 'packets', which are then transmitted separately, often through different routes, to the recipient, where the message is reassembled. It follows that in order to intercept a given communication that is travelling over the internet (say, an email), any intercepting agency will need to obtain all the packets associated with that communication, and reassemble them*" (§1.30).

15. This characterisation of Upstream was recently endorsed by the Independent Reviewer of Terrorism, David Anderson QC (the "Independent Reviewer"), in his report on the bulk powers provided for in the Investigatory Powers Bill, which is currently being debated by the UK Parliament.[54] Indeed, the Independent Reviewer states that "*[t]he bulk interception power in the Bill…is very similar to the s702 [FISA] power*" and that "*it is not wholly accurate to suggest…that the US has turned away from bulk*" for "*[t]he s702 arrangements continue to permit the targeted selection and retention by the NSA of wanted communications from bulk internet traffic*".[55] It is also worth noting that the Independent Reviewer observed that "*[t]he broadly-phrased Executive Order 12333…implicitly authorises an extremely wide range of techniques for use outside the USA, whereby data may be acquired in bulk*".[56]

16. Even at the filtering stage, it is not entirely clear whether Upstream can be fairly described as a "targeted" program. The NSA has not fully declassified

to Dismiss the First Amendment Complaint, *Wikimedia v. NSA*, No. 15-cv-00662 (D. Md. Aug. 6, 2015)). Nevertheless, the Applicants assert that the legal implications remain the same in either scenario as the companies are being compelled to act at the government's behest.

[54] DAVID ANDERSON Q.C., INDEPENDENT REVIEWER OF TERRORISM LEGISLATION, REPORT OF THE BULK POWERS REVIEW, August 2016, *available at* https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf ("Bulk Powers Review").

[55] Bulk Powers Review, §§3.64-3.65. The UK Government has made clear that the bulk interception power in the Investigatory Powers Bill will "*replace the power to intercept 'external communications' in Chapter 1, Part 1 of RIPA*", which includes s. 8(4). *See* Investigatory Powers Bill: Explanatory Notes, 8 June 2016, para 16, *available at* http://www.publications.parliament.uk/pa/bills/lbill/2016-2017/0040/17040en.pdf.

[56] Bulk Powers Review, §§3.65(c).

its procedures governing the process by which persons may be targeted under section 702. Selectors cannot be key words "*such as 'bomb' or 'attack" or "the names of targeted individuals*", but beyond these constraints, as with the s8(4) Regime, the full scope of permissible selectors is not known (see Applicants' Reply, paras 43-47).[57] Again, while the common examples are email addresses and telephone numbers, it might be possible, for example, for a selector to include an IP address (or a range of IP addresses), servers, gateways or cable heads, which may capture the information of many people.[58]

17. In addition, during the filtering process, Upstream captures "*multiple communications transactions*", which is "*an Internet 'transaction' that contains more than one discrete communication within it.*"[59] In a declassified 3 October 2011 opinion of the Foreign Intelligence Surveillance Court, Judge John Bates observed that, in practice, "*due to the technological challenges associated with acquiring Internet transactions,*" Upstream is "*generally incapable of distinguishing between transactions containing only a single discrete communication…and transactions containing multiple discrete communications, not all of which may be to, from, or about a tasked selector.*"[60] He concluded that given "*the sheer volume of transactions acquired by NSA through its upstream collection…the Court cannot know for certain…the number of non-target communications acquired*".[61]

[57] PCLOB, s702 report, p 33.

[58] As the UK Government itself has recognised, many people can use the same IP address: "*[T]here are only a limited number of IP addresses on the internet. This means that companies providing internet access will sometimes need to share IP addresses between a large number of different devices at the same time.*" Home Office, Operational Case for the Retention of Internet Connection Records, p 9, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473769/Internet_Connection_Records_Evidence_Base.pdf.

[59] PCLOB, s702 report, p 7.

[60] [Redacted], 2011 WL 10945618 (FISA Ct. Oct. 3, 2011), pp 30-31 *available at* https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf ("FISC Opinion").

[61] FISC Opinion, pp 31-32.

18. Finally, the Upstream filtering process uses to, from and "about" selectors. An "about" selector is one "*contained within the communication*" even where "*the targeted person is not necessarily a participant in the communication*."[62] The inclusion of "about" selectors may therefore ensnare a wider range of information.[63] Thus, for all the reasons canvassed above, it remains possible that filtering in Upstream might also be characterised as "bulk", in that it captures the communications of individuals for whom the government lacks reasonable suspicion that such individuals have committed or are committing a criminal offence or are a threat to national security.

19. As for PRISM, the Applicants acknowledge that the Snowden disclosures originally, and erroneously, indicated that the US Government had direct access to the servers of US internet companies.[64] It now appears that the US Government "*(specifically, the FBI on behalf of the NSA) sends selectors…to a United States-based electronic communications service provider*", which is then "*compelled to give the communications sent to or from that selector to the government*".[65] Nevertheless, the same concerns regarding the scope of selectors in Upstream apply equally to PRISM.

[62] PCLOB, s702 report, p 7.

[63] The use of *about* selectors also raises additional privacy concerns as it enhances the scope of intrusion at the filtering stage. In order to determine whether a communication is "about" a particular selector, Upstream must search the content of all extracted information. The ACLU has accordingly characterised this practice as "*the digital analogue of having a government agent open every piece of mail that comes through the post to determine whether it mentions a particular word or phrase*". First Amended Complaint, *Wikimedia v. NSA*, No. 15-cv-00662 (D. Md. June 19, 2015), para 50, *available at* https://www.aclu.org/legal-document/wikimedia-v-nsa-first-amended-complaint-declaratory-and-injunctive-relief.

[64] *See* Barton Gellman & Ashkan Soltani, *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, THE WASHINGTON POST, 7 June 2013, https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (cited in King Witness Statement, para 51); Glenn Greenwald & Ewen MacAskill, *NSA Prism program taps in to user data of Apple, Google and others*, THE GUARDIAN, 7 June 2013, https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (cited in King Witness Statement, para 51).

[65] PCLOB s702 report, p 33.