

On Behalf Of: The Applicants
Name: C. Cohn
Number: First
Exhibits: CC1
Date: 27 September 2013

Application No: 58170/13

IN THE EUROPEAN COURT OF HUMAN RIGHTS

B E T W E E N :

- (1) BIG BROTHER WATCH;
- (2) OPEN RIGHTS GROUP;
- (3) ENGLISH PEN; AND
- (4) DR CONSTANZE KURZ

Applicants

- v -

UNITED KINGDOM

Respondent

WITNESS STATEMENT OF
CINDY COHN

I, Cindy Cohn, of Electronic Frontier Foundation, 815 Eddy Street, San Francisco, California 94109 USA will say as follows:

INTRODUCTION

1. I am the Legal Director of the Electronic Frontier Foundation (“EFF”) as well as its General Counsel, positions I have held since September 2000. EFF is the leading civil liberties Non-Governmental Organisation focusing on digital technologies, defending free speech, privacy and innovation online. EFF has over 24,000 dues paying members around the world, including in the European Union and has been active since 1990, trying to build a better,

more just and more free Internet for all, through impact litigation, policy advocacy and public participation.

2. I have particular expertise in the field of national security and surveillance for intelligence purposes. In this field, I have been lead attorney in a number of proceedings in United States courts since 1993, and have also testified before the Congress of the United States. I am also currently lead counsel in *Jewel v. National Security Agency*, a case concerning the dragnet surveillance of communications within the United States by the United States' National Security Agency ("**NSA**") and counsel in *First Unitarian Church v. National Security Agency*, which challenges the collection of bulk phone records by the NSA, also known as the Associational Tracking Program.
3. Where the contents of this statement are within my knowledge, I confirm that they are true; where they are not, I have identified the source of the relevant information, and I confirm that they are true to the best of my knowledge and belief.
4. I make this statement in support of the application brought by the Applicants to the European Court of Human Rights. In doing so, I set out background information for the Court in relation to:
 - 4.1. The disclosures of information which have taken place thus far in the United States in relation to the NSA's "§702" programmes (PRISM and UPSTREAM);
 - 4.2. The admissions made by the United States' government in relation to those programmes to date;
 - 4.3. An overview of the legal basis for the programmes under United States law; and
 - 4.4. Weaknesses in the United States' regime of privacy protection and legal challenges to it.
 - 4.5. I also address further disclosures of information which relate to the mass collection of telephone calling records of persons located in the United States ("the Associational Tracking Program"), under section 215 of the Patriot Act.

5. In examining the government programmes as they have been described by the United States government and/or the NSA I in no way intend to endorse them, nor do I necessarily accept or assert that the programmes are actually being implemented as described. In many places with regard to these rapidly unfolding revelations, the public only has vague assertions and conclusory defences from the government about what they are doing, why they are doing it and whether they are following their own rules in practice. EFF has repeatedly called upon the United States Congress to initiate a fully independent, empowered investigation into the spying being done by the NSA¹ and any other government agencies. EFF also has Freedom of Information Act requests pending². My goal in this statement is to provide this Court with such publicly available information as exists, as well as government explanations as I know them and as the government has admitted to date. It is not, and cannot be, to provide a complete recitation of the facts, since many facts are simply not known to the public and the story continues to unfold. Finally, none of these assertions should be taken as admissions or legal conclusions or in any other way as statements by any EFF clients.
6. There is now produced and shown to me a paginated bundle of true copy documents marked "CC1". All references to documents in this statement are to Bundle CC1 unless otherwise stated, in the form [CC1/Tab/Page].

PRISM and UPSTREAM (aka §702 Programmes)

7. PRISM is the name of an internal government computer system³ established and implemented by the NSA [CC1/1/pp.99-101]. It enables the NSA to access metadata and internet content from some of the largest internet service providers in the United States (and the world) and other companies providing communications services, including Microsoft, Yahoo, Google, and Facebook.

¹ See "In Response to the NSA, We Need A New Church Committee and We Need It Now", C. Cohn and T. Timm, 7 June 2013, available at <https://www.eff.org/deeplinks/2013/06/response-nsa-we-need-new-church-commission-and-we-need-it-now> (last accessed, 11 September 2013).

² See "Hundreds of Pages of NSA Spying Documents to be Released As Result of EFF Lawsuit", T. Timm, 5 September 2013, available at <https://www.eff.org/deeplinks/2013/09/hundreds-pages-nsa-spying-documents-be-released-result-eff-lawsuit> (last accessed, 11 September 2013).

³ "Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act", Director of National Intelligence, 7 June 2013, available at <http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/871-facts-on-the-collection-of-intelligence-pursuant-to-section-702-of-the-foreign-intelligence-surveillance-act> (last accessed, 18 September 2013).

8. UPSTREAM is a government programme established by the NSA to copy all traffic passing through the fibre optic cables of United States communications services providers, such as AT&T and Verizon.
9. Between them, PRISM and UPSTREAM provide very broad access to the communications content and metadata of non-United States Persons.⁴ They provide for the bulk seizure, acquisition, collection and storage of all or nearly all of the communications content and metadata of non-United States persons that passes through the United States. They also provide for various kinds of searching and analysis of that content and metadata with little or no restriction, both to determine whether content is related to a US person. Moreover, they appear to provide for additional searching and analysis of the content and metadata once the material is determined not to be related to a United States person; or where it has been determined that it does relate to a United States person, but subject to one of many exceptions to the general exclusion of searching of data relating to United States persons. The government claims that both programmes are authorised under Section 702 of the *Foreign Intelligence Surveillance Act 1978* (“**FISA**”) (as amended by the *Foreign Intelligence Surveillance Amendment Act 2008* (“**FISAAA**”), 50 U.S.C. § 1881a (“**§702**”) [**CC1/2/pp.304-314**]. Other surveillance programmes are authorised by §702, likely including many that have not yet been made public, but for purposes of this witness statement, I will refer to PRISM and UPSTREAM collectively as “§702 programmes” or “programmes.”
10. Because of the network structure of the Internet -- which now carries a tremendous amount of telephone calls as well as what is conventionally thought of as “Internet” traffic such as email, web activity, social networking, chat and others - PRISM and UPSTREAM together allow NSA access to a tremendous amount of non-United States Persons’ communications and metadata⁵ [**CC1/1/pp.102-105**]. For instance, for just metadata, the ‘Boundless Informant’ documents published by *The Guardian* on 11 June 2013 show the agency

⁴ Under the FISA law, 50 U.S.C. §1801 (i) “United States person” means “a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101 (a)(20) of title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.”

⁵ “*Using Domestic Networks to Spy on the World*,” Katitza Rodriguez and Tamir Israel, available at <https://www.eff.org/deeplinks/2013/06/spies-without-borders-i-using-domestic-networks-spy-world> (last accessed, 11 September 2013).

collecting almost 3 billion pieces of intelligence from United States computer networks over a 30-day period ending in March 2013⁶ [CC1/1/pp.106-110]. A 2010 Washington Post article discussing content and metadata reported that "every day, collection systems at the [NSA] intercept and store 1.7bn emails, phone calls and other type of communications"⁷ [CC1/1/pp.114-119].

11. A key feature of these programmes is that they do not respond to specific operations or investigations, but are designed as broad, *a priori* authorisations for the NSA to collect a wide range of data concerning non-United States persons (as I will identify below in light of the legal framework). As explained further below, all of the processes put into place for the programmes are apparently aimed at ensuring protection for the communications of United States persons which, despite being *collected* along with those of non-United States persons, at home or abroad, and at least preliminarily analysed will only in certain situations be more deeply analysed, used or distributed by the NSA. Much of the discussion in the United States is about whether those steps are sufficient to accord with the legal protections in United States law of United States persons, but notably, for these purposes, none of those protections or processes are aimed at protecting non-suspect, innocent non-United States persons from having their communications or communications records collected or searched by the NSA or transferred to other countries.

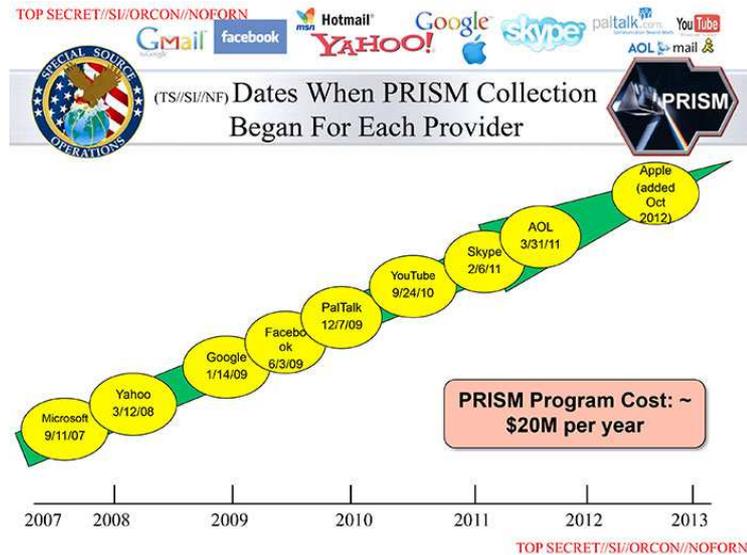
12. The PRISM programme was first revealed through newspaper reports in *The Guardian* and *The Washington Post* on 6 June 2013. These reports were based on disclosures to those newspapers by the former defence contractor employee Edward Snowden. The reports exposed the NSA's practice of "collect[ing data] directly from the servers"⁸ of nine leading United States Internet companies, including Microsoft, Google, Yahoo, Facebook and Apple. These companies had begun their cooperation with the NSA when Microsoft first joined the programme on 11 September 2007. A timeline of this cooperation recording the

⁶ "Boundless Informant: The NSA's Secret Tool To Track Global Surveillance Data," Glenn Greenwald and Ewan MacAskill, theguardian.com, Tuesday 11 June 2013 14.00 BST, available at <http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining>; see also "How the NSA is still harvesting your online data," Glenn Greenwald and Spencer Ackerman, theguardian.com, Thursday 27 June 2013 16.03 BST available at <http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection> (last accessed, 19 September 2013).

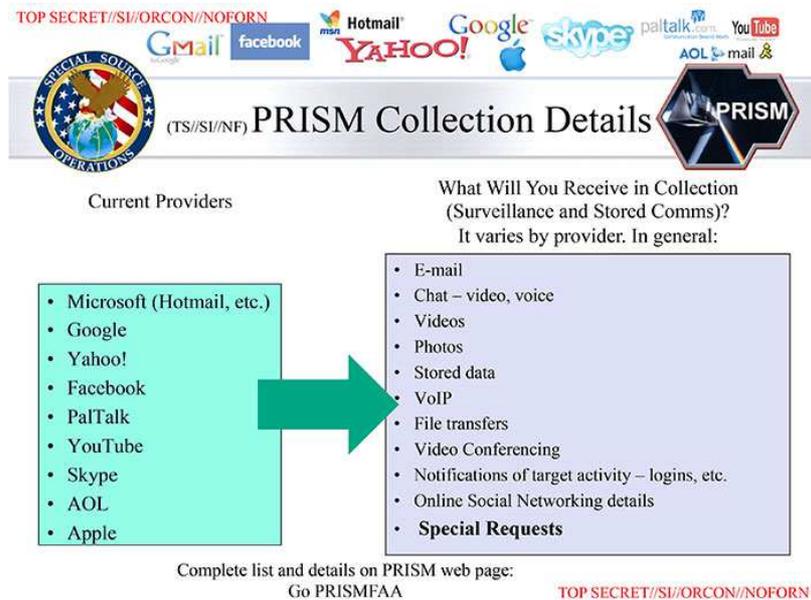
⁷ "Top Secret America: A Hidden World, Growing Beyond Control," Dana Priest and William M. Arkin, available at <http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/3/> (last accessed, 19 September 2013).

⁸ See slide on page 8.

programme's annual cost to the NSA was set out in an internal NSA slide from April 2013 published by the newspapers:



13. According to the slide, through PRISM the NSA is able to “[c]ollect[data] directly” from U.S. service providers’ servers and extract audio and video chats, photographs, e-mails, documents, and connection logs that enable analysts to track foreign targets as well as phone calls [CC11/p.122-130]⁹:



⁹ “U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program”, Barton Gellman and Laura Poitras, http://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 (last accessed, 11 September 2013) [CC11/pp.120-121C].

14. A helpful description of the operation of the system was provided by *The Washington Post* [CC1/1/pp.131-133], in light of information from insiders with experience of the programme:

“According to slides describing the mechanics of the system, PRISM works as follows: NSA employees engage the system by typing queries from their desks. For queries involving stored communications, the queries pass first through the FBI’s electronic communications surveillance unit, which reviews the search terms to ensure there are no U.S. citizens named as targets.

That unit then sends the query to the FBI’s data intercept technology unit, which connects to equipment at the Internet company and passes the results to the NSA.

The system is most often used for e-mails, but it handles chat, video, images, documents and other files as well”¹⁰.

15. The scale of the operation is probably unprecedented. *The Guardian’s* reports noted that over 2,000 Prism-based “reports” of communications were being issued every month by the NSA and that more than 77,000 intelligence reports had been made by June 2013 [CC1/1/pp.134-140]¹¹.

16. The UPSTREAM programme copies traffic flowing through the United States Internet system and then runs it through a series of filters. These filters are designed to sift for communications that involve at least one person outside the United States and that may be of foreign-intelligence value, or that are subject to one of the other exceptions such as being encrypted or revealing a crime.

17. The Wall Street Journal reported [CC1/1/pp.141-145] that:

“[...] there are two common methods used, according to people familiar with the system. In one, a fiber-optic line is split at a junction, and traffic is copied to a processing system that interacts with the NSA’s systems, sifting through information based on NSA parameters. In another, companies program their routers to do initial filtering based on metadata from Internet “packets” and send copied data along. This data flow goes to a processing system that uses NSA parameters to narrow down the data further.”¹²

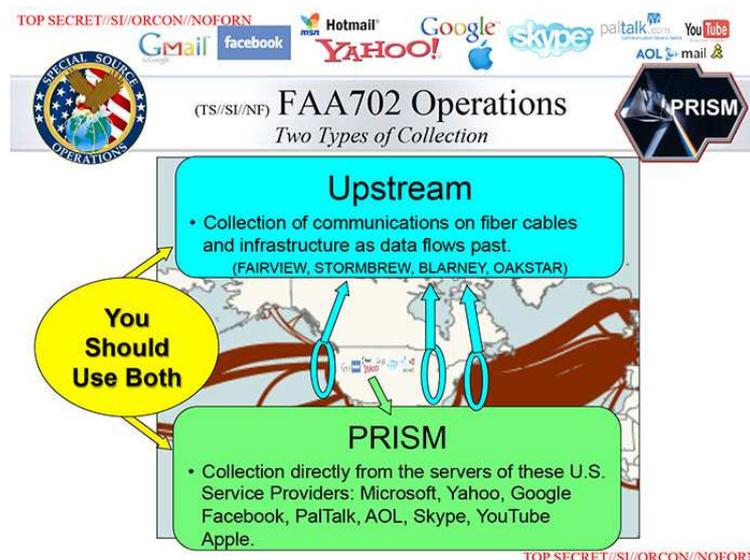
¹⁰ U.S., company officials: *Internet surveillance does not indiscriminately mine data*, 8 June 2013, http://www.washingtonpost.com/world/national-security/us-company-officials-internet-surveillance-does-not-indiscriminately-mine-data/2013/06/08/5b3bb234-d07d-11e2-9f1a-1a7cdee20287_story_1.html (last accessed, 18 September 2013).

¹¹ “NSA Prism program taps in to user data of Apple, Google and others”, Glenn Greenwald and Ewen MacAskill, *The Guardian*, Friday 7 June 2013, available at <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> (last accessed, 18 September 2013).

¹² “What You Need to Know on New Details of NSA Spying,” Jennifer Valentino-Devries and Siobhan Gorman, 20 August 2013, 8:12 p.m. ET, available at

18. The existence of the UPSTREAM programme was first exposed by AT&T Whistleblower Mark Klein¹³ in 2006 and is the basis of EFF's *Jewel v. NSA* lawsuit, pending since 2008¹⁴. It was also the basis of an earlier case, *Hepting v. AT&T*, which was brought directly against AT&T but dismissed after Congress passed retroactive immunity for the companies assisting NSA in 2008¹⁵. The UPSTREAM programme gives the NSA a copy of all content and metadata of all communications travelling over the fibre-optic cables of major American telecommunications carriers.

19. The PRISM and UPSTREAM programs are both used by the NSA to collect information from the United States' Internet infrastructure and between them, they give access to nearly all traffic traveling over or stored by the infrastructure. Indeed, the April 2013 Slides instruct NSA personnel to make full use of both programmes:



20. The names “Fairview, Stormbrew, Blarney and Oakstar” reportedly refer to codenames of the surveillance programmes linked to each participating major telecommunications company in the U.S. including Verizon, AT&T and Sprint¹⁶ [CC1/1/pp.146-150].

<http://online.wsj.com/article/SB10001424127887324108204579025222244858490.html>

(last accessed, 19 September 2013).

¹³ Declaration of Mark Klein, available at <https://www.eff.org/node/55051>.

¹⁴ Jewel v. NSA Case page: available at <https://www.eff.org/cases/jewel>.

¹⁵ Hepting v. NSA Case page: available at <https://www.eff.org/nsa/hepting>.

¹⁶ “New Details Show Broader NSA Surveillance Reach” Jennifer Valentino-Devries and Siobhan Gorman, 20 August 2013, 11:31 p.m. ET, available at <http://online.wsj.com/article/SB10001424127887324108204579022874091732470.html#project%3DNSA0820%26articleTabs%3Darticle> (last accessed, 11 September 2013).

The role of private companies

21. Initially, the internet companies concerned with PRISM publicly denied that they were aware of such a programme [CC1/1/pp.151-153]¹⁷. However, since that time some of these companies have acknowledged its existence (if not by that name, which appears to be an internal governmental system codename) and their knowledge of it, while denying that some of the processes work as described in the slides [CC1/1/pp.131-133]¹⁸ Google has stated publicly that it supplies information to the NSA pursuant to PRISM by transferring data to a secure FTP (File Transfer Protocol), such as a secure “dropbox”, or in person, rather than United States authorities having direct access to its servers [CC1/1/pp.154-156]¹⁹. *The Guardian* has also reported that United States-based companies which take part in the programme have been paid significant sums to cover the cost of complying with requests for access to their information [CC1/1/pp.157-161]²⁰.
22. During the months of June and July 2013, several of the companies involved in PRISM, namely AOL, Apple, Facebook, Google, Microsoft, and Yahoo filed petitions to the Foreign Intelligence Surveillance (or “FISA”) Court, seeking to have reporting restrictions on the programme lifted [CC1/1/pp.162-163]²¹. The Internet companies have filed cases in the FISA court to follow up on these requests, which have not been granted.²²

¹⁷ “PRISM scandal: tech giants flatly deny allowing NSA direct access to servers”, Nicholas Rushe and James Ball, New York, guardian.co.uk, Friday 7 June 2013 00.48 BST, <http://www.guardian.co.uk/world/2013/jun/07/prism-tech-giants-shock-nsa-data-mining> (last accessed, 8 September 2013).

¹⁸ “U.S., company officials: Internet surveillance does not indiscriminately mine data”, 8 June 2013, http://www.washingtonpost.com/world/national-security/us-company-officials-internet-surveillance-does-not-indiscriminately-mine-data/2013/06/08/5b3bb234-d07d-11e2-9f1a-1a7cdee20287_story_1.html (last accessed, 8 September 2013).

¹⁹ “Google’s real secret spy program? Secure FTP”, Kim Getter, Wired.com 11 June 2013, available at <http://www.wired.com/threatlevel/2013/06/google-uses-secure-ftp-to-feds/>.

²⁰ “NSA paid millions to cover Prism compliance costs for tech companies”, Ewen MacAskill, The Guardian, Friday 23 August 2013, available at <http://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid> (last accessed, 8 September 2013).

²¹ “Just Like Google, Microsoft Formally Challenges Data Disclosure Gag Order”, Mike Isaac, 26 June 2013, available at <http://allthingsd.com/20130626/just-like-google-microsoft-formally-challenges-data-disclosure-gag-order/>.

²² See, e.g. Google’s entry on its official blog on 9 September 2013, available at <http://googleblog.blogspot.com/2013/09/petition-for-greater-transparency.html> (last accessed, 11 September 2013); or Yahoo’s announcement of its petition on the same day, “Yahoo files lawsuit against NSA over user data”, Ewen MacAskill in New York, theguardian.com, Monday 9 September 2013 21.09 BST, available at <http://www.theguardian.com/world/2013/sep/09/yahoo-lawsuit-nsa-surveillance-requests> (last accessed, 11 September 2013).

23. Accordingly, these companies – as well as civil liberties groups (including the American Civil Liberties Union (ACLU) and EFF) – have written to the President and the leaders of the United States Senate and House of Representatives demanding that they be allowed to publish data about secret demands for user data [CC1/1/p.164]²³. To date, I am not aware of any resolution of this request. However, on 29 August 2013, James Clapper (the Director of National Intelligence (“DNI”)) pledged that going forward the Executive would disclose annual reports with at least some sort of aggregate numbers of FISA orders issued to technology and telecommunications companies. It is not clear how useful those numbers will be to the public in assessing the scale and lawfulness of the programmes.
24. As far as I am aware, the telecommunications companies like Verizon and AT&T and Sprint who are participating in the UPSTREAM programme have not formally and publicly confirmed their participation in those specific programmes, nor have they sought permission to provide further information to the public.
25. The Wall Street Journal published the following graphic which sets out a helpful overview of the operation of these programmes²⁴:

²³ “Microsoft Asks Attorney General to Intervene in Request to Disclose PRISM Info”, [Arik Hesseldahl](http://allthingsd.com/20130716/microsoft-asks-attorney-general-to-intervene-in-request-to-disclose-prism-info/), 16 July 2013, available at <http://allthingsd.com/20130716/microsoft-asks-attorney-general-to-intervene-in-request-to-disclose-prism-info/> (last accessed, 8 September 2013).

²⁴ Available at <http://online.wsj.com/article/SB10001424127887324108204579022874091732470.html#project%3DNSA0820%26articleTabs%3Dinteractive>.

How the NSA Scours Internet Traffic in the U.S.

The National Security Agency gathers information from many sources. Here are three main ones—with a focus on one way it can tap and study Internet traffic.

○ Select red dots for more information

Data collected from sources

The NSA gets much of its communication information from companies

Phones

The NSA can gather phone-call data. ○



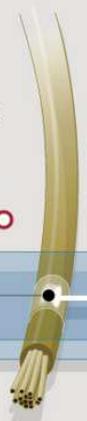
Prism

Stored content from Internet firms, aimed at foreign targets. ○



Internet backbone

Monitors certain streams of Internet traffic, through legal relationships with telecom companies. ○



Internet data sorted

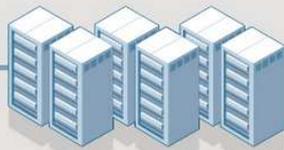
The NSA filters out the data it needs

Filtering System

Companies such as Narus make technology that filters large streams of Internet traffic. The system aims at communications where at least one person is overseas. ○

Main databases

Data goes into NSA databases. ○



Information might also go to an analyst for study in real time.

NSA Processing

Systems including one called Xkeyscore take 'selectors,' such as email addresses sent by analysts, develop filtering rules and send information back. ○

Query programs

Software for analysts to spot links or patterns in piles of data. ○



Analyst

Gives instructions to the filtering algorithms, gets information from databases and studies the data.



Reports

Final reports are stored in databases named Maui and Anchovy.



Sources: current and former U.S. and industry officials; documents revealed by Edward Snowden

The Wall Street Journal

ADMISSIONS BY THE UNITED STATES GOVERNMENT

26. Since the newspaper disclosures, the United States government has publicly acknowledged the existence of the PRISM and UPSTREAM §702 programmes and provided information about their operation. On 6 June 2013, the DNI confirmed PRISM's existence and explained that it was authorised under FISAAA [CC1/1/pp.196-201]²⁵.

²⁵ "U.S. Confirms That It Gathers Online Data Overseas", Charlie Savage, Edward Wyatt and Peter Baker, June 6, 2013, New York Times, http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html?pagewanted=all&_r=0 (last accessed, 11 September 2013).

27. On 21 August 2013, the DNI declassified two FISA court rulings confirming the existence of both §702 programmes, and explaining problems with the UPSTREAM programme.²⁶ Notably for these purposes, the problems arose from the retention and searching of United States persons' information. The bulk seizure, collection, search and analysis of the communications and communications records of non-United States persons was not questioned or limited by these decisions.

28. On 8 June 2013, the DNI provided a 'fact sheet' on the programmes, setting out the Executive's understanding of their purpose and limits [CC1/1/pp.99-101]²⁷. The fact sheet stated, in summary:

- PRISM is an internal government computer system used to facilitate the government's statutorily authorised collection of foreign intelligence information from electronic communication service providers under court supervision, as authorised by section 702 of FISA.
- Section 702 facilitates the targeted acquisition of foreign intelligence information concerning foreign targets located outside the United States, under court oversight. Service providers supply information to the Government when they are lawfully required to do so. Under section 702 of FISA, the United States Government does not unilaterally obtain information from the servers of U.S. electronic communication service providers. All such information is obtained with FISA Court approval and with the knowledge of the provider based upon a written 'Directive' from the Attorney General and the DNI.
- In order to obtain authorisation under section 702 the Government needs to document that the purpose of the acquisition is the prevention of terrorism, hostile cyber activities, or nuclear proliferation, or another appropriate foreign intelligence purpose and the foreign target is reasonably believed to be outside the United States.
- Section 702 cannot be used to intentionally target any United States citizen, or any other United States person, or to intentionally target any person known to be in the United States. Likewise, Section 702 cannot be used to target a person outside the

²⁶ These files are available at <http://www.dni.gov/files/documents/October%202011%20Bates%20Opinion%20and%20Order%20Part%201.pdf> and <http://www.dni.gov/files/documents/September%202012%20Bates%20Opinion%20and%20Order.pdf> (last accessed, 11 September 2013).

²⁷ See note 3 above.

United States if the purpose is to acquire information from a person inside the United States.

29. The fact sheet stated that the collection of intelligence information under section 702 is subject to an oversight regime, incorporating reviews by the executive, legislative and judicial branches. As to the judicial branch, the fact sheet states:

“All FISA collection, including collection under Section 702, is overseen and monitored by the FISA Court [FISC], a specially established Federal court comprised of 11 Federal judges appointed by the Chief Justice of the United States.

The FISC must approve targeting and minimization procedures under Section 702 prior to the acquisition of any surveillance information.

- *Targeting procedures are designed to ensure that an acquisition targets non-U.S. persons reasonably believed to be outside the United States for specific purposes, and also that it does not intentionally acquire a communication when all the parties are known to be inside the US.*
- *Minimization procedures govern how the Intelligence Community (IC) treats the information concerning any U.S. persons whose communications might be incidentally intercepted and regulate the handling of any nonpublic information concerning U.S. persons that is acquired, including whether information concerning a U.S. person can be disseminated. Significantly, the dissemination of information about U.S. persons is expressly prohibited unless it is necessary to understand foreign intelligence or assess its importance, is evidence of a crime, or indicates a threat of death or serious bodily harm.”*

It is notable, for the purposes of this case, that the “minimization” procedures which are applied by the FISC are only concerned with ensuring minimal use and discarding of the data of United States-persons after initial analysis and searching.

30. On 7 June 2013, President Obama also made a statement to journalists with regard to the programme [CC1/1/pp.202-207]:

“[] the programs that have been discussed over the last couple days in the press are secret in the sense that they’re classified, but they’re not secret in the sense that when it comes to telephone calls, every member of Congress has been briefed on this program.

With respect to all these programs, the relevant intelligence committees are fully briefed on these programs. These are programs that have been authorized by broad, bipartisan majorities repeatedly since 2006. And so I think at the outset, it’s important to understand that your duly elected representatives have been consistently informed on exactly what we’re doing.

*Now, with respect to the Internet and emails, this does not apply to U.S. citizens, and it does not apply to people living in the United States. And again, in this instance, not only is Congress fully apprised of it, but what is also true is that the FISA Court has to authorize it.*²⁸

31. In a public hearing of the House's Intelligence Committee in Washington on 18 June 2013, the NSA's Director, Keith Alexander, also acknowledged the programme's existence. He asserted that it was "*critical*" to the effectiveness of United States intelligence and had "*helped prevent more than fifty*" terrorist attacks in over twenty countries. He described the programme as "*limited, focused and subject to rigorous oversight*". The Deputy Attorney General, James Cole, told the Committee that the NSA (a) sends an "*aggregate number*" of times it has searched the database to the FISA court every 30 days and (b) reports every occasion on which NSA analysts inappropriately searched the database [CC1/1/pp.208-2010]²⁹. He noted that "[e]very now and then, there may be a mistake" [CC1/1/pp.211-212C]. An internal audit by the NSA disclosed a month later also recorded an instance in which the NSA did not report an inappropriate search³⁰.
32. At a press conference in Berlin on 18 June 2013, President Obama again confirmed the existence of the programme. He defended the United States' legal regime, stating that it "*applies very narrowly to leads [the United States] ha[s] obtained to issues relating to terrorism and proliferation of weapons of mass destruction. [...] Based on those leads with court supervision and oversight we can access information*" [CC1/1/p.213]³¹. He also referenced the "*fifty cases*" in which potential attacks against the United States and other countries had been averted as a result of the use of the programme.

²⁸ "*Transcript: Obama's Remarks on NSA Controversy*", June 7, 2013, available at <http://blogs.wsj.com/washwire/2013/06/07/transcript-what-obama-said-on-nsa-controversy/> (last accessed, 8 September 2013).

²⁹ "*NSA chief claims 'focused' surveillance disrupted more than 50 terror plots*", Spencer Ackerman, The Guardian, Wednesday 19 June 2013, available at <http://www.theguardian.com/world/2013/jun/18/nsa-surveillance-limited-focused-hearing> (last accessed, 8 September 2013).

³⁰ "*NSA broke privacy rules thousands of times per year, audit finds*", Barton Gellman, August 15, 2013, available at http://articles.washingtonpost.com/2013-08-15/world/41431831_1_washington-post-national-security-agency-documents (last accessed, 8 September 2013).

³¹ "*Barack Obama Justifies Prism NSA Surveillance Programme, Saying It Has Saved Lives*", Huffington Post UK, By Christopher York, 19 June 2013, posted at 13:32 BST, available at http://www.huffingtonpost.co.uk/2013/06/19/prism-obama-germany-merkel_n_3464613.html.

THE LEGAL ISSUES RELATED TO THE PROGRAMMES

33. The standard rule under United States law is that the intentional interception, use, or disclosure of wire and electronic communications is prohibited unless a statutory exception applies. See Title III of the *Omnibus Crime Control and Safe Streets Act 1968* (Pub. L. 90-351, 82 Stat. 197 (codified as amended at 18 U.S.C. §§ 2510-2522)) [CC1/2/pp.261-267]. In general, these prohibitions bar third parties (including the government and private intermediaries such as communications service providers) from wiretapping telephones and installing electronic "sniffers" that read Internet traffic (18 U.S.C. § 2511(1)).

34. In two decisions decided in 1967, the United States Supreme Court held that wiretaps and similar intrusions into privacy were subject to the Fourth Amendment to the United States Constitution (*Katz v United States* 389 US 347 (1967) [CC1/2/pp.360-389]; and *Berger v New York*, 388 US 41 (1967) [CC1/2/pp.390-479]). The Fourth Amendment provides that:

“Amendment IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

35. In *Katz v United States*, the Court applied the Fourth Amendment to the interception of telephone calls:

“The Government urges that, because its agents relied upon the decisions in *Olmstead* and *Goldman*, and because they did no more here than they might properly have done with prior judicial sanction, we should retroactively validate their conduct. That we cannot do. It is apparent that the agents in this case acted with restraint. Yet the inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer. They were not required, before commencing the search, to present their estimate of probable cause for detached scrutiny by a neutral magistrate. They were not compelled, during the conduct of the search itself, to observe precise limits established in advance by a specific court order. Nor were they directed, after the search had been completed, to notify the authorizing magistrate in detail of all that had been seized. In the absence of such safeguards, this Court has never sustained a search upon the sole ground that officers reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive means consistent with that end.”³²

36. However, there are two key ways that the government can be relieved of this general prohibition against the interception of communications. First, when authorised by the Justice Department and signed by a United States District Court or Court of Appeals judge, a

³² Pages 356-357 [CC1/2/p.370].

wiretap order permits domestic law enforcement, such as the FBI, to intercept communications of named individuals or premises for up to thirty days for certain identified domestic law enforcement purposes (18 U.S.C. §§ 2516(1), 2518(5)). 18 U.S.C. §§ 2516-2518 imposes several formidable requirements that must be satisfied before investigators can obtain a Title III order. Most importantly, the application for the order must show “*probable cause*” to believe that the interception will reveal evidence of predicate federal felonies. 18 U.S.C. §2516(3).

37. A second method is via FISA, which allows interception of communications, again largely by the FBI for national security purposes. FISA processes are described further below. Section 702 FISA represents a particularly clear departure from the standard rule, given that it establishes a mechanism of *a priori* authorisations of untargeted surveillance, rather than being directed at specific individuals or identifiers like email addresses or phone numbers. Essentially, as a matter of United States law, the communications and metadata of non-United States persons generally can be intercepted and analysed with very few limitations.

38. I will briefly set out the background to FISA and its key features before examining in detail the relevant statutory provisions.

The background to §702 FISA

39. FISA authorises the acquisition of foreign intelligence data, generally differentiating between *collection* inside and outside the United States as well as *persons* inside and outside the United States. Applications for court orders authorising searches or surveillance under FISA are made to the secret FISA Court, which consists of eleven District Court judges selected by the Chief Justice of the United States Supreme Court (as to which see below). Applications are made by the Department of Justice, usually on behalf of the FBI, under oath by a federal officer with the approval of the Attorney General, the Acting Attorney General, or the Deputy Attorney General. (50 U.S.C. §§ 1801(g), 1804, 1823). The application must identify or describe the target of the search or surveillance, and establish that the target is either a “*foreign power*” or an “*agent of a foreign power*” (50 U.S.C. §§ 1804(a)(3), 1804(a)(4)(A), 1823(a)(3), 1823(a)(4)(A)). A “*foreign power*” is defined to include, among other things, a “*foreign government or any component thereof*” and a “*group engaged in international terrorism*” (50 U.S.C. §§ 1801(a)(1), (4)). The purpose of the tap must be to obtain foreign intelligence (although this need only be a “*significant*” and not

necessarily the “*primary*” purpose (50 U.S.C. § 1805(a)(2)).

40. Unlike wiretap processes, which are generally required to be disclosed to the targets after the wiretap concludes (although that disclosure can be delayed and can be subject to suppression motions in domestic prosecutions), FISA Court proceedings are conducted in private and its rulings are not published – unless they are declassified by the Executive branch. There had been only a handful of declassifications until those specified above, which were made in response to the recent revelations in the press. Except in the rare circumstance of a prosecution that relies on FISA-collected information and in which the government decides to disclose that fact, the ‘targets’ of proposed intelligence operations are not informed of this process, and then only after the fact, and so are generally unable to challenge it.

41. Several United States courts have rejected constitutional challenges to FISA as applied to non-bulk acquisition of communications³³.

42. In *United States v Duggan*, 743 F. 2d 59 (2d Cir. 1984) at page 73 [CC1/2/pp.480-507], the Second Circuit held that although Amendment IV affords protection to non-United States citizens, Congress is not prevented “*from adopting standards and procedures that are more beneficial to United States citizens and resident aliens than to non-resident aliens, so long as the differences are reasonable*”.

43. The public rationale behind the enactment of FISA 702 is put starkly by the United States Justice Department, in light of that default position, as follows:

“Before the enactment of [s. 702], in order to conduct the kind of surveillance authorized by section 702, FISA was interpreted to require that the Government show on an individualized basis, with respect to all non-U.S. person targets located overseas, that there was probable cause to believe that the target was a foreign power or an agent of a foreign power, and to obtain an order from the [FISA Court] approving the surveillance on this basis. In effect, the Intelligence Community treated non-U.S. persons located overseas like persons in the United States, even though foreigners outside the United States generally are not entitled to the protections of the Fourth Amendment. Although FISA’s original procedures are proper for electronic surveillance of persons inside this country, such a process for surveillance of terrorist suspects overseas can slow, or even prevent, the Government’s acquisition of vital information,

³³ See e.g. *United States v Hassan Abu-Jihaad*, 630 F. 3d 102, 120 (2d Cir. Dec. 20, 2010) and cases cited therein.

without enhancing the privacy interests of Americans. Since its enactment in 2008, section 702 has significantly increased the Government's ability to act quickly³⁴.

Section 702 FISA

44. Section 702 FISA was introduced by the **FISAAA [CC1/2/pp.302-344]**. This provision allows the Attorney General (“**AG**”) and the DNI jointly to authorise, for up to one year “*the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information*”: s. 702(a) FISA, 50 USC §1881a [**CC1/2/p.287**]. The provision of a general authorisation is to be distinguished from the process of obtaining a specific, targeted warrant as described above. In particular, an application for an authorisation does not need to “*identify the specific facilities, places, premises, or property at which an acquisition authorized [...] will be directed or conducted*” (s.702(g)(4)).

45. Section 702 addresses targeting, but as recent revelations have confirmed, with the exception of the prohibition on the intentional acquisition of the communications of United States persons, it creates few, if any restrictions on the seizure or collection of the communications and communications records of non-United States persons.

Requirements

46. Section 702(a) provides:

“(a) Authorization

Notwithstanding any other provision of law, upon the issuance of an order in accordance with subsection (i)(3) or a determination under subsection (c)(2), the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.”

47. The principal method for securing an authorisation under FISA section 702(a) is by obtaining an order under subsection 702(i)(3). Subsection 702(i)(3) provides that an order approving the surveillance can be made if it is submitted with a “*written certification and any supporting affidavit, under oath and under seal*” in accordance with subsection 702(g).

48. The requirements of subsection 702(g) are as follows [**CC1/2/pp.290-291**]:

“(2) REQUIREMENTS.—A certification made under this subsection shall—

³⁴ James R Clapper and Eric H Holder, ‘Background Paper on Title VII of FISA Prepared by the Department of Justice and the Office of Director of National Intelligence’ 8 February 2012, available at <http://www.justice.gov/ola/views-letters/112/02-08-12-fisa-reauthorization.pdf>, (last accessed 15 August 2013) [**CC1/1/pp.214-221**].

(A) attest that—

(i) there are procedures in place that have been approved, have been submitted for approval, or will be submitted with the certification for approval by the Foreign Intelligence Surveillance Court that are reasonably designed to—

(I) ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and

(II) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States;

(ii) the minimization procedures to be used with respect to such acquisition—

(I) meet the definition of minimization procedures under section 101(h) or 301(4), as appropriate; and

(II) have been approved, have been submitted for approval, or will be submitted with the certification for approval by the Foreign Intelligence Surveillance Court;

(iii) guidelines have been adopted in accordance with subsection (f) to ensure compliance with the limitations in subsection (b) and to ensure that an application for a court order is filed as required by this Act;

(iv) the procedures and guidelines referred to in clauses (i), (ii), and (iii) are consistent with the requirements of the fourth amendment to the Constitution of the United States;

(v) a significant purpose of the acquisition is to obtain foreign intelligence information;

(vi) the acquisition involves obtaining foreign intelligence information from or with the assistance of an electronic communication service provider; and

(vii) the acquisition complies with the limitations in subsection (b);

(B) include the procedures adopted in accordance with subsections (d) and (e);

(C) be supported, as appropriate, by the affidavit of any appropriate official in the area of national security who is—

(i) appointed by the President, by and with the advice and consent of the Senate; or

(ii) the head of an element of the intelligence community;

(D) include—

(i) an effective date for the authorization that is at least 30 days after the submission of the written certification to the court; or

(ii) if the acquisition has begun or the effective date is less than 30 days after the submission of the written certification to the court, the date the acquisition began or the effective date for the acquisition; and

(E) if the Attorney General and the Director of National Intelligence make a determination under subsection (c)(2), include a statement that such determination has been made.

[...]

(4) Limitation

A certification made under this subsection is not required to identify the specific facilities, places, premises, or property at which an acquisition authorized under subsection (a) will be directed or conducted.”

49. The “targeting” procedures that have to be complied with are described in subsection 702(d) as procedures adopted by the AG in consultation with the DNI that are reasonably designed to:

“(A) ensure that any acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and
(B) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.”

50. The “minimization” procedures which also have to be in place are also described in subsection (e) as procedures adopted by the AG in consultation with the DNI. A document dated 31 October 2011 setting out these procedures has since been declassified [CC1/2/pp.222-234]³⁵. In summary:

- Personnel are required to exercise “*reasonable judgment in determining whether information acquired must be minimized*” and must “*destroy inadvertently acquired communications of or concerning a United States person at the earliest practicable point in the processing cycle*” (s.3(b)(1));
- Communications – even if they are those of ‘United States persons’, inadvertently obtained – may be retained for up to “*five years from the expiration date of the certification authorizing the collection*” (s.3(b)(1)). However, where communications are identified as being “*domestic*” they must be destroyed immediately unless the DNI specifically instructs their retention for one of several listed purposes (Section 5);
- Personnel are expected to sift through discrete communications and identify relevant material; and
- The document specifically recognises the ability of the NSA to disseminate information obtained pursuant to s.702 FISA to “*a foreign government*” (s.8(a)) subject only to limitations on the dissemination of information about United States persons (s.6(b)) and the requirements of any other applicable law (s.7).

51. The second way of obtaining an authorisation under FISA section 702(a) is in cases of emergency. The authorisation can be implemented by reference to subsection (c)(2), which provides that the AG and the DNI may begin gathering information before obtaining a court order where they make a “*determination*” that: “*exigent circumstances exist* [which mean that] *without immediate implementation of an authorization under subsection (a), intelligence*

³⁵ The relevant material can be found on the DNI’s website, available at <http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf>.

important to the national security of the United States may be lost or not timely acquired and time does not permit the issuance of an order". In such a case they may apply for *post hoc* court approval at a later time (s. 702(i)(3)(A)), although this must be within seven days of the determination (s.702(g)(1)(B)).

52. If the Court finds the certification to be compliant, then the Court must enter an order approving the authorisation (s. 702(i)(3)(A)). Intelligence may then be gathered for the period specified in the authorisation.

Limitations

53. FISA section 702(b) includes general limitations on the exercise of the power:

“(b) Limitations

An acquisition authorized under subsection (a)—

- (1) may not intentionally target any person known at the time of acquisition to be located in the United States;
- (2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;
- (3) may not intentionally target a United States person reasonably believed to be located outside the United States;
- (4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and
- (5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.”

54. However, as is clear, these limitations are only designed to ensure that information concerning United States persons is not obtained through the use of the section 702 powers. It is with this objective in mind that the AG and DNI are required (s.702(g)(2)(a) FISA) to certify the ‘*targeting procedures*’ (s.702(d) FISA) and ‘*minimisation procedures*’ (s.702(e) FISA) before seeking an authorisation. Any acquisition of intelligence must also comply with these procedures (s.702(c)(1)(A)). However, given that the focus of any review (see paragraph 59 below) would be compliance with these statutory tests, the Court does not approve or review any *specific acquisitions* of intelligence -- it merely approves procedures for acquisition and minimisation and relies upon the Agency to self-report any misuse or problems in implementation of these general procedures. Furthermore, it is possible that such “targeting” may be of communications or other facilities, and not of specific individuals or entities.

55. Therefore, in summary, section 702 authorisation at least allows the following to be obtained from or with the assistance of an electronic communications provider, stored and searched:

- targeted information against a person outside the United States unless they are a “*United States person*” or the target is a United States person where one or more recipients of a communication are outside the United States;
- non-targeted information in bulk where one or more recipients of communications are outside the United States as long as the actual target is not a United States person;
- data on United States persons or persons inside the United States so long as this is an unintended by-product of an authorisation, where the person is not the target, not based solely on a person’s exercise of his or her First Amendment rights and is held for a permitted purpose;

The government does not need to name the specific facilities, places, premises, or property at which an acquisition authorised will be directed or conducted when it asks the FISA Court to certify the lawfulness of the proposed targeting and minimisation procedures that apply to directives issued under section 702.

The use of private providers’ services

56. Section 702 envisages that the acquisition of information will be obtained “*from or with the assistance of an electronic communication service provider*” (s.702(g)(2)(A)(vi)) i.e. in collaboration with private companies. This takes place through the use of “Directives” given by the NSA to electronic communication service providers to provide “*all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition.*” (s. 702(h)(1)(A)). These Directives may be given to telecommunications providers subject to U.S. jurisdiction, only. The NSA has stated that it considers this “*the most significant tool in the NSA collection arsenal for the detection, identification, and disruption of terrorist threats to the United States and around the world*”³⁶. It appears that this collaboration formed the backbone of the PRISM and UPSTREAM programmes.

57. The AG can ask the FISA Court for an order compelling a provider that refuses to comply

³⁶ National Security Agency, ‘*The National Security Agency: Missions, Authorities, Oversight and Partnerships*’, 9 August 2013 http://www.nytimes.com/interactive/2013/08/10/us/politics/10obama-surveillance-documents.html?hp&_r=0#document/p24 (last accessed 15 August 2013).

with a request for production of requested information (s. 702(h)(5)(A)). However, an electronic communications service provider may also apply for the order to be set aside or modified by the Court (s. 702(h)(4)(A)).

Review mechanisms

58. The legislative regime's envisaged review mechanisms are as follows:

58.1. The AG, in consultation with the DNI, must adopt guidelines to ensure targeting and minimisation procedures are respected (s. 702(f)(1)). These guidelines must be provided to Congressional intelligence committees, the Congressional committees on the judiciary, and the FISA Court (s. 702(f)(2)).

58.2. At least every six months, the AG and the DNI are to self-assess compliance with the targeting and minimisation procedures and with the guidelines. They must submit their self-assessment to the Congressional intelligence committees and the Congressional committees on the judiciary. In a letter to the House and Senate Leadership arguing for reauthorisation of s. 702, the DNI and the AG stated that the Department of Justice and the Office of the Director of National Intelligence "*conduct extensive oversight reviews of s. 702 activities every 60 days*".³⁷

58.3. The Inspector-General of the Department of Justice and the Inspectors-General of the intelligence agencies authorised to acquire foreign intelligence information under s. 702 must self-review the number of reports that contain a reference to a United States citizen or resident of the United States and the number of targets that were determined after they had been targeted to actually be within the United States. The results of these self-reviews are to be provided to the AG, the DNI, the Congressional intelligence committees and the Congressional committees on the judiciary (s. 702(l)(2)). The same review must be done on an annual basis by the head of each intelligence agency that acquires foreign intelligence information under s. 702 (s. 702(l)(3)).

59. Private communications providers are able to appeal rulings by the FISA Court to the Foreign Intelligence Surveillance Court of Review (the "**FISA Review Court**") (s.702(h)(6)(A)), which is comprised of three judges also designated by the Chief Justice.

³⁷ See James R Clapper and Eric H Holder, Background paper, n.34 above.

Rulings of the FISA Review Court can be appealed to the Supreme Court of the United States (s.702(h)(6)(B)).

60. As is clear, however, these reviews are aimed only at ensuring that the analysis, search and other uses of communications does not concern information regarding United States citizens or persons in the United States outside the permitted scope of such uses.

Weaknesses in the FISA regime

61. There has been significant criticism of the FISA regime on a number of fronts: (i) the secrecy of the FISA Court's procedure (ii) the lack of effective oversight by that Court of Executive action (iii) and the potential and actual breadth of surveillance under the statutory regime.

Secrecy of the process

62. As I noted above, the procedure before the FISA Court is secretive and is not normally subjected to public scrutiny. The only exception has been where the Executive has chosen to declassify FISA Court Opinions. This had rarely occurred until the President requested that disclosures be made following the public revelations in June 2013. The DNI disclosed a range of material including FISA Court decisions on 21 August 2013³⁸. One of these decisions (dated 3 October 2011) was disclosed as an example of the FISA Court's exercise of powers of oversight of the NSA's activities. In that decision, the Court found that one aspect of the NSA's upstream collection of Internet transactions had breached the statutory requirements of FISA (certain minimisation procedures were not sufficiently stringent) and violated Amendment IV of the Constitution. The Order referenced several other Orders, however, which were not released, nor were the governmental submissions that led to the Order. The Order itself was also redacted in key areas.

63. In a cover letter to those disclosures [CC1/1/pp.235-238], the DNI defended the regime, and asserted that the materials disclosed demonstrated not only the effectiveness of the NSA's *internal* checks and balances, but also the Court's supervision³⁹. However, as noted below at paragraph 64, the Chief Judge of that Court has publicly cast doubt on the assertions of adequate Court supervision and a later audit report from the intelligence agencies

³⁸ These documents are available at <http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/915-dni-declassifies-intelligence-community-documents-regarding-collection-under-section-702-of-the-foreign-intelligence-surveillance-act-fisa>.

³⁹ Cover Letter, 21 August 2013, available at <http://www.fas.org/irp/news/2013/08/dni082113.pdf>.

demonstrated far more problems than the DNI and the President had let the public to believe (see paragraph 68 below).

64. One proposal which has been made is the introduction of special 'privacy advocates' to the FISA Court's proceedings, charged with representing the interests of targeted persons and upholding constitutional and statutory guarantees [CC1/1/pp.239-241]⁴⁰. Others have suggested changing the selection process for the Court to obtain a more balanced cross-section of the Judiciary than the current process, where the Chief Justice of the Supreme Court makes the selections. Other reform proposals have also been raised. To date, it is unclear whether any of these proposals will be adopted.

The absence of effective oversight

65. The effectiveness of the FISA court's oversight has been subjected to sustained challenge since the disclosures by *The Guardian* and *The Washington Post*. In a written statement given to *The Washington Post* in August 2013, the Chief Judge of the FISA Court, United States District Judge Reggie B. Walton, stated that the court's oversight was limited, given that "[t]he FISC is forced to rely upon the accuracy of the information that is provided to the Court [...], it] does not have the capacity to investigate issues of noncompliance, and in that respect the FISC is in the same position as any other court when it comes to enforcing [government] compliance with its orders" [CC1/1/pp.242-244]⁴¹.
66. There has been no evidence that the FISA Court has prospectively denied authorisations to the surveillance authorities since its inception, but only that on several occasions it has requested adjustments of certain aspects of authorisation requests (as in the case of the 3 October 2011 Opinion). The FISA Court works closely and interactively with the executive branch on these proposals and, in the opinion of former Judge Robertson, it acts more like an administrative agency than a court [CC1/1pp.245-246]⁴².

⁴⁰ "US senators push for special privacy advocate in overhauled FISA court", Spencer Ackerman, theguardian.com, Thursday 1 August 2013 18.38 BST, available at <http://www.theguardian.com/law/2013/aug/01/fisa-court-bill-us-senate>.

⁴¹ "Court: Ability To Police U.S. Spying Program Limited", Carol D. Leonnig (with Barton Gellman, Peter Wallsten and Alice Crites), published: August 16 2013, available at http://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125_print.html.

⁴² "Former judge admits flaws with secret FISA court," Associated Press, 9 July 2013, http://www.cbsnews.com/8301-250_162-57592836/former-judge-admits-flaws-with-secret-fisa-court/ (last accessed, 11 September 2013)..

The breadth of the surveillance

67. The focus of much domestic criticism of the breadth of surveillance through section 702 programmes in the United States has been the potential effects on United States persons as a result of these surveillance programmes. Even if the §702 programme surveillance works as asserted by the Government, it admittedly includes the bulk seizure and collection of the communications and communications records of United States persons, which simply was not at issue in any of the previous judicial rulings concerning FISA. The United States Constitution addresses both the seizure and search of the “papers” of Americans, which includes their electronic communications, so there are serious questions about whether these programmes violate the Constitution.
68. Additionally, the §702 programme surveillance allows the storage and search of United States persons’ communications and communications records upon an administrative guess that there is a 51% chance that a person is not a United States person, and allows communications and communications records to be stored and searched if they merely “about” a target, are encrypted or if there is evidence of a crime, among other exceptions, even if they are to or from a United States person or purely domestic. It also appears that the NSA is providing tips to other agencies and instructing them to hide the fact that the information came from the programme surveillance⁴³ [CC1/1/pp.247-248]. All of these issues have raised strong concerns inside the United States.
69. Moreover, there are concerns that the programme even as adopted is not being administered in a way that protects the privacy of United States persons. An internal NSA Audit from May 2012 disclosed by *The Washington Post* recorded that the PRISM programme has been used for significant unauthorised surveillance (for instance, of United States communications), with the NSA breaching privacy rules thousands of times a year, in the face of repeated assurances from the President and other senior intelligence figures of the effectiveness of the system [CC1/1/pp.211-212]⁴⁴.
70. Prior to the recent revelations of bulk surveillance, a direct challenge to the constitutionality

⁴³ “DEA and NSA Team Up to Share Intelligence, Leading to Secret Use of Surveillance in Ordinary Investigations,” Hanni Fakhoury, 6 August 2013, <https://www.eff.org/deeplinks/2013/08/dea-and-nsa-team-intelligence-laundering> (last accessed, 19 September 2013).

⁴⁴ See “NSA broke privacy rules thousands of times per year, audit finds”, at note 30 above.

of FISAAA was brought in the *Clapper v Amnesty International USA* case (in particular in light of its breadth) (No 11-1025, slip op (Sup Ct, Feb 26, 2013)). However, the complainants were denied standing, as they claimed to have been targeted and the majority of the Court held that only persons who could actually prove that they had been targeted and that their communications had been targeted would be able to bring that form of constitutional challenge.

71. Although the White House initially opposed moves to curb NSA surveillance⁴⁵ [CC1/1/pp.249-252], President Obama has since expressed some support for reforms of the current regime, accepting that "[w]e need new thinking for a new era"⁴⁶ [CC1/1/pp.253-256]. However he has not released any details and instead the Department of Justice has been strongly defending the current regime in the courts and the Intelligence Community has been strongly defending it in public fora.

Legal Challenges to the PRISM and UPSTREAM §702 Programmes

72. Since 2006, I have handled a case challenging the UPSTREAM programme as in violation of both statutory restrictions and Amendments I and IV of the U.S. Constitution. It is called *Jewel v. NSA*.⁴⁷ The suit is pending in the Federal District Court for the Northern District of California and seeks an injunction and damages against the NSA, Justice Department, FBI and directors of the agencies to stop the "*illegal and unconstitutional program of dragnet electronic surveillance*". It also seeks damages allowable under law. The Court recently rejected the government's claim that the case had to be dismissed due to the State Secrets privilege and also found that the FISA law procedures of 1806(f) applied and pre-empted the state secrets privilege⁴⁸. The matter returns to Court on September 27, 2013.

73. A class-action suit has also been filed in Washington DC against both the government and against the internet companies involved in the § 702 programmes including Microsoft, AOL,

⁴⁵ *White House urges Congress to reject moves to curb NSA surveillance*, Spencer Ackerman, theguardian.com, 24 July 2013, available at <http://www.guardian.co.uk/world/2013/jul/24/nsa-surveillance-amash-amendment> (last accessed, 8 September 2013).

⁴⁶ *Obama touts NSA surveillance reforms to quell growing unease over programs*, Paul Lewis and Spencer Ackerman, The Guardian, Friday 9 August 2013 22.16 BST, available at <http://www.theguardian.com/world/2013/aug/09/obama-nsa-surveillance-reforms-press-conference>.

⁴⁷ A significant purpose of the acquisition is to obtain foreign intelligence information; see the case summary at <https://www.eff.org/cases/jewel>.

⁴⁸ This process allows the protection of information which is deemed by the government to be sensitive national security information in the course of consideration of whether the surveillance was legal, see <https://www.eff.org/node/74895>.

Facebook, Google and Apple⁴⁹ [CC1/1/pp.257-258]. The action seeks \$20 billion in damages and attorney fees and an injunction ending the PRISM programme.

74. Several other cases are also pending relating to the telephone records collection programmes discussed further below. However, as is clear from the matters set out above, there has been no significant judicial or legislative challenge in the United States courts to the breadth of the surveillance of non-United States persons.

75. On Wednesday 11 September 2013 the CEO of Facebook, Mark Zuckerberg, stated that the government had done a "*bad job*" of balancing the right of non-United States persons to privacy and its duty to protect, noting that the government response of "*Oh don't worry, we're not spying on any Americans*" was not "*going to inspire confidence in American internet companies*"⁵⁰.

THE COLLECTION AND SEARCHING OF DOMESTIC TELEPHONE RECORDS IN THE UNITED STATES

76. Another dimension of the NSA's programmes which has been the focus of litigation and news reports alongside the §702 programmes is the acquisition of the telephone records of persons *in* the United States from telecommunications providers under s.215 of the PATRIOT ACT [CC1/2/pp.301A-301G].

77. Section 215 allows collection of "tangible things" within the U.S., so long as they are relevant to an investigation concerning "*foreign intelligence information*" and relating to a non-United States citizen, or more narrowly concerning "*international terrorism*" and relating to a U.S. citizen (s.215(a)(1)) [CC1/2/pp.301F-301G]. The government claims that "[*tangible item*" can include telephone records in electronic storage and that the telephone records of all

⁴⁹ "PRISM Class-Action Lawsuit Filed: \$20B, Injunction Sought Against 'Complicit' Companies and Officials Lawsuit says Obama chilled free speech; attorney encourages citizens to 'man the barricades of freedom'", Steven Nelson, June 12, 2013 available at <http://www.usnews.com/news/newsgram/articles/2013/06/12/prism-class-action-lawsuit-filed-20b-injunction-sought-against-complicit-companies-and-officials>.

⁵⁰ "Zuckerberg: US government 'blew it' on NSA surveillance", Dominic Rushe in San Francisco, theguardian.com, Thursday 12 September 2013 01.18 BST, available at <http://www.theguardian.com/technology/2013/sep/11/yahoo-ceo-mayer-jail-nsa-surveillance> (last accessed, 19 September 2013).

Americans are “relevant” to its investigations.⁵¹ These assertions are the subject of intense debate both in the courts and outside them⁵². For instance, EFF has filed a brief on behalf of the key author of the PATRIOT Act, Representative Sensenbrenner, asserting that the government’s interpretation is incorrect.⁵³

78. The FISA Court appears to have interpreted the relevance standard and “tangible things” broadly to permit acquisition of all telephone records of all Americans. An example of such a wide authorisation is an April 2013 order of a former member of the FISA Court, Roger Vinson, ordering Verizon to provide the NSA with the phone records of all its customers for a 90-day period⁵⁴. The government has stated that this bulk collection of telephone records has been going on for years and that the April 2013 order was renewed for another 90-day period.

79. The exercise of this power has been the subject of litigation by EFF, in a case entitled *First Unitarian Church of Los Angeles v. NSA*⁵⁵ and the ACLU in a case entitled *ACLU v. Clapper*⁵⁶, as well as by the Electronic Privacy Information Center (EPIC) in a writ petition to the U.S. Supreme Court entitled *In Re Electronic Privacy Information Center*. These cases raise statutory concerns as well as concerns under the First and Fourth Amendment. EFF calls the programs the “Associational Tracking Programs” to highlight the First Amendment concerns with the NSA having access to all of the communications of Associations ranging from churches to political activist groups to groups that give legal assistance.

80. Additionally EFF and the ACLU have pending FOIA cases seeking transparency about the various FISC decisions and government actions around both 702 and 215. There have been recent developments in these cases, and it is likely that the FISA court’s reasoning on them

⁵¹ See US Justice Department ‘*Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA Patriot Act*’ (9 August 2013), available at <http://www.nytimes.com/interactive/2013/08/10/us/politics/10obama-surveillance-documents.html?hp#document/p1> (last accessed, 15 August 2013).

⁵² For an overview of ACLU’s brief in *ACLU v. Clapper* see <https://www.aclu.org/files/pdfs/natsec/clapper/2013.08.26%20ACLU%20PI%20Brief.pdf>. See also “*The Criminal NSA*,” Jennifer Granick and Christopher Sprigman, available at http://www.nytimes.com/2013/06/28/opinion/the-criminal-nsa.html?pagewanted=all&_r=0

⁵³ For a copy of EFF’s amicus brief see <https://www.eff.org/document/aclu-v-clapper-amicus-brief>.

⁵⁴ “*NSA collecting phone records of millions of Verizon customers daily*,” Glenn Greenwald, *The Guardian*, Thursday 6 June 2013, available at <http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>.

⁵⁵ <https://www.eff.org/cases/first-unitarian-church-los-angeles-v-nsa>.

⁵⁶ <https://www.aclu.org/national-security/aclu-v-clapper-challenge-nsa-mass-phone-call-tracking>.

may soon become public⁵⁷.

81. In late July 2013, a legislative measure was proposed by Justin Amash, a Michigan Republican Representative which would stop the NSA acquiring the telephone records of millions of Americans without suspicion of a crime. The amendment to the *Defence Appropriations Bill 2014* sought to prevent, the FBI and other agencies from relying on Section 215 of the Patriot Act "to collect records, including telephone call records, that pertain to persons who are not subject to an investigation under Section 215."⁵⁸ This proposal was ultimately defeated in a close vote in the House of Representatives, but more than a dozen other bills seeking various kinds of reform of the NSA Spying are currently pending in Congress.

CONCLUSION

82. The scale of these intelligence programmes is unprecedented and has caused significant public debate and scrutiny of the practices of the United States Surveillance Agencies. It is also clear that there have been and will likely continue to be many legislative and judicial challenges to the lawfulness of PRISM and the other programmes used by the NSA.

However, it is also clear that there is very little engagement in the courts and legislature in the United States and in the Obama Administration's defence of the surveillance, with the lack of restrictions on the bulk surveillance of foreign communications, even where these merely pass through the United States or where they concern non-suspect, innocent non-United States persons. Given that non-United States persons will not have knowledge of the fact that their communications are being intercepted, and in any event do not have any recourse against this surveillance as a matter of constitutional and statutory law in the United States this is an issue which is unlikely to be resolved in the United States' courts.

⁵⁷ On Friday September 13 2013, Judge Dennis Saylor of the FISA Court ruled that the American Civil Liberties Union and its co-litigants had the right to seek disclosure of the Fisa court's interpretations of section 215 of the Patriot Act - <http://www.theguardian.com/world/2013/sep/13/edward-snowden-nsa-disclosures-judge> (last accessed, 14 September 2013).

⁵⁸ "House forces vote on amendment that would limit NSA bulk surveillance Opposition to bulk surveillance swells with vote that would 'end authority for blanket collection of records under the Patriot Act'", Spencer Ackerman, [theguardian.com](http://www.theguardian.com), Tuesday 23 July 2013 20.26 BST <http://www.guardian.co.uk/world/2013/jul/23/house-amendment-nsa-bulk-surveillance>.

STATEMENT OF TRUTH

I believe that the facts stated in this Witness Statement are true.

SIGNED:


.....
Cindy Corn

DATE:

27 Sept 2013

Application No: 58170/13

IN THE EUROPEAN COURT OF HUMAN
RIGHTS

BETWEEN:

- (1) BIG BROTHER WATCH;
- (2) OPEN RIGHTS GROUP;
- (3) ENGLISH PEN; AND
- (4) DR CONSTANZE KURZ

Applicants

- v -

UNITED KINGDOM

Respondent

WITNESS STATEMENT OF
CINDY COHN

Deighton Pierce Glynn Solicitors

Centre Gate
Colston Avenue
Bristol BS1 4TR

Tel: 0117 317 8133

Fax: 0117 317 8093

www.deightonpierceglynnc.co.uk