On Behalf Of: The Applicants
Name: C. Cohn
Number: Second
Exhibit: CC2
Date: 2 March 2015

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

SECOND 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. This is my second witness statement in these proceedings. 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.

2. I make this second statement in order to update the Court regarding the US Government's communications surveillance activities and regulatory framework. It is structured as follows (which, generally speaking, follows the order of my first statement):

   2.1. Section I sets out the further information that is now in the public domain regarding the PRISM and UPSTREAM programs. This illustrates the extensive material gathered by the US government and which may be accessed by the UK intelligence services. I also provide further published evidence regarding the UK's own TEMPORA program;

   2.2. Section II then identifies the further information that has now been leaked regarding other similar programs run by the US and UK intelligence services. Most importantly, this information shows the extensive access to UK databases that has been granted by the UK government to the US government; and

   2.3. Section III tracks developments in Government transparency, reform initiatives, and legal challenges in the wake of these disclosures. Most importantly, these are of very limited, or no, application to persons outside the United States.

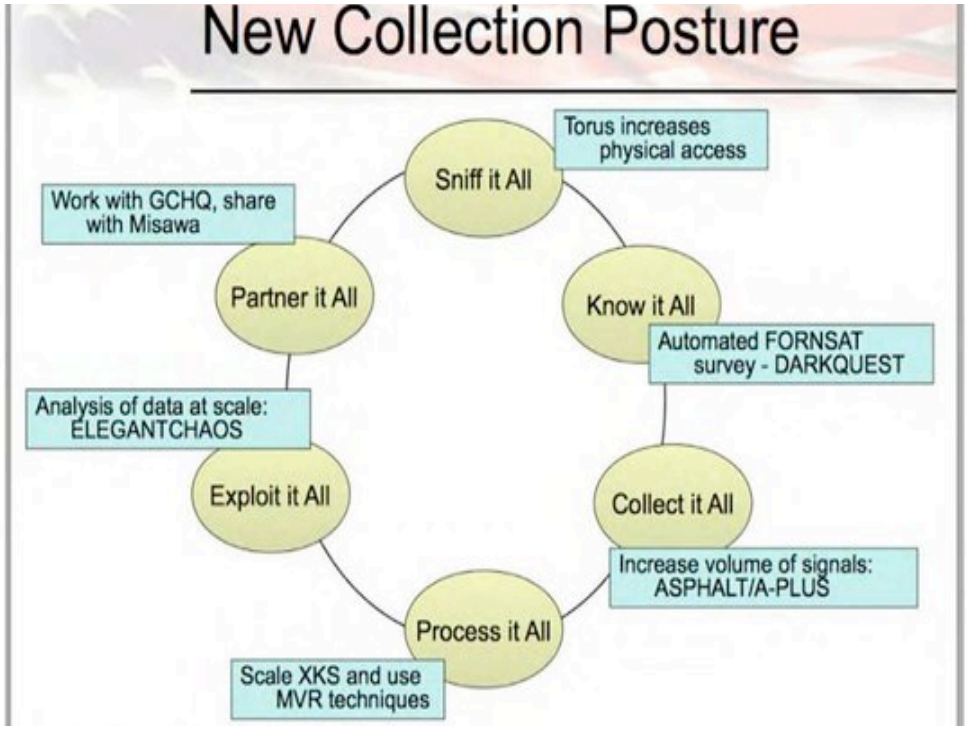
3. There is now produced and shown to me a paginated bundle of true copy documents marked "CC2". All references to documents in this statement are to Bundle CC2 unless otherwise stated, in the form [**CC2/Page**].

Section I: UPDATE ON PRISM AND UPSTREAM (aka §702 Programs) AND TEMPORA

4. In my first witness statement, I described the operation of the PRISM and UPSTREAM programs, implemented under section 702 of Foreign Intelligence Surveillance Act 1978 ("FISA"), and their co-option of private internet and telecommunications companies' infrastructure. Some further details have now emerged about the way these programs function, in particular the way in which the data of non-suspect, non-US persons and of American citizens' data is captured alongside data relating to targeted persons, who the US government claims are all non-US persons.

5. This additional information is important because it highlights the massive numbers of innocent Europeans whose communications are swept up and analysed by the NSA and, likely, transmitted to the United Kingdom. In short, the additional information confirms that the NSA's surveillance is massively disproportionate in its reach, particularly given the US government's public position that none of the limitations on collection apply to non-US persons.

6. The clearest illustration of the NSA's disproportionate approach to collection of non-US persons' information is contained in this PowerPoint slide, which the NSA showed at a 2011 meeting of the Five Eyes, an intelligence alliance of the US, the United Kingdom, Canada, Australia, and New Zealand.[1]



The "collection posture" is assumed to summarise the US government's intentions regarding PRISM and UPSTREAM and other similar programs. The aim is to "Collect it All", to both "Process" and "Exploit" all of that material and, as regards UK access to this material, "to Partner it All".

[1] Available with the materials for Glenn Greenwald's book, *No Place to Hide*: http://hbpub.vo.llnwd.net/o16/video/olmk/holt/greenwald/NoPlaceToHide-Documents-Uncompressed.pdf#page=5,

7. This additional information also highlights one of the key ways in which the NSA's public descriptions of its surveillance can be misleading: when the NSA is referencing who it *targets* for surveillance, it is not describing all those who have had their communications and communications records collected, analysed, and shared by the NSA with foreign partners (including GCHQ). The NSA's targets are a small subset of the communications it has reviewed (as noted below the Washington Post's review indicates that approximately 90% of the analysis is of non-targets). Further, those who are targeted are only a small percentage of those collected and at least initially analysed by the NSA.

8. This conclusion has been buttressed by journalists who have reviewed not just the information or records collected, but the *content of communications* actually analysed by the NSA. For instance, on 5 July 2014, in an article entitled "*In NSA-intercepted data, those not targeted far outnumber the foreigners who are*"[2] (Exhibit CC2/Pages 1-12) the Washington Post reported that "*ordinary internet users, American and non-American alike*" far outnumbered the legally targeted foreigners in the communications intercepted by the National Security Agency ("NSA") pursuant to programs such as PRISM and UPSTREAM. The Post had analysed a large cache of intercepted conversations which had been provided by Edward Snowden to the newspaper. The conversations had been obtained by the NSA pursuant to FISA s702 authorisations. Around 160,000 intercepted e-mail and instant message conversations and 7,900 documents taken from 11,000 online accounts were reviewed. The newspaper found that nine of ten account holders were not the intended surveillance targets but were "*caught in a net the agency had cast for somebody else*". The article acknowledges that valuable intelligence was contained in the emails, but drew attention to the wealth of material regarding "*sexual liaisons, mental-health crises, political and religious conversions and financial anxieties*". The report also estimated that of the nearly 90,000 targets authorised under s702 FISA, the number of persons whose communications will have been intercepted and retained will at least ten times higher.

9. The Washington Post report also noted the often superficial designations of targets as "foreign" (and thus able to be targeted under s702 FISA):

[2] http://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html

"*One analyst rests her claim that a target is foreign on the fact that his e-mails are written in a foreign language, a quality shared by tens of millions of Americans. Others are allowed to presume that anyone on the chat "buddy list" of a known foreign national is also foreign*"

10. At paragraph 49 of my first witness statement I referred to the targeting procedures used in connection with the interception of communications relating to foreign persons under s702 FISA. Although now replaced, a leaked version of the former targeting procedures, dated 22 July 2009 has been released[3], which I exhibit at Exhibit CC2/Pages 13-22. These show that the NSA continues to treat non-US persons as having no privacy protections against s702 collection. The NSA takes a similar position for largely non-US collection under Executive Order 12333, discussed further below.

11. The procedures also show that persons were assumed to be non-US persons unless positively shown otherwise (p.4):

"*in the absence of specific information regarding whether a target is a United States person, a person reasonably believed to be located outside the United States or whose location is not known will be presumed to be a non-United States person unless such person can be positively identified as a United States person, or the nature or circumstances of the person's communications give rise to a reasonable belief that such person is a United States person*."

They also show that the FISA Court permitted the NSA to make use of information 'inadvertently' collected from domestic US communications without a warrant.

12. The sum total of these disclosures is to reaffirm that non-US persons have no protection against NSA collection, analysis, and use of their communications and communications records. Thus, to the extent that this information is given to GCHQ, there is no indication that any privacy or other protections have been applied to the information of or about European citizens.

13. Since my first witness statement there have also been disclosures regarding the US's use of GCHQ programs such as TEMPORA[4]. On 18 June 2014, Der Spiegel published a large cache of documents regarding German intelligence services' cooperation with

[3] http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document
[4] http://www.spiegel.de/international/germany/new-snowden-revelations-on-nsa-spying-in-germany-a-975441.html

the US government. This included US briefing notes on PRISM as well as their use of UK-operated programs such as TEMPORA, which are of course at the heart of this Application. I exhibit the key documents hereto at Exhibit CC2/Pages 23-52:

13.1. An NSA document dated 19 September 2012 (Exhibit CC2/Pages 33-36) describes TEMPORA as "*more than 10 times larger than the next biggest XKEYSCORE [the NSA's computer system for searching and analysing intercepted internet data] …This massive site [TEMPORA] uses over 1000 machines to process and make available to analysts more than 40 billion pieces of content a day*." It describes TEMPORA as "*GCHQ's 'Internet buffer' which exploits the most valuable Internet links available to GCHQ*"

13.2. Another document extract referred to permitting the German security services access to XKeyscore (Exhibit CC2/Page 41);

13.3. The last exhibited document describes refers to 197 PRISM-based reports for GCHQ from mid-2011 to mid-2012 (Exhibit CC2/Pages 49-51). This corresponds with the reported number referred to by Ian Brown in his previous Witness Statement in these proceedings at paragraph 45.

Section II: ADDITIONAL LEAKED DISCLOSURES and EXECUTIVE ORDER 12333

14. In addition to further developments regarding the US Government's PRISM and UPSTREAM programs and GCHQ's TEMPORA program, new disclosures have been made in the press regarding the operation of other similar programs.

15. Most importantly for this Application, on 30 October 2013, the Washington Post reported that the NSA had tapped the internal communications links of Internet giants like Yahoo and Google in order to intercept communications in an unencrypted format and without the participation of the providers (Exhibit CC2/Pages 53-60)[5]. A leaked document dated January 2013 recorded that over the previous 30 days, field collectors had intercepted and sent to the NSA 181,280,466 new records, including both content and metadata.

[5] http://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

The tool used to carry out the interception was called MUSCULAR. It was reported that it was "*operated jointly with [GCHQ]*". The report noted that:

> "*the infiltration is especially striking because the NSA, under a separate program known as PRISM, has front-door access to Google and Yahoo user accounts through a court-approved process*."

Describing GCHQ's role further, the Post reported that "*GCHQ directs all intake into a 'buffer' that can hold 3-5 days of traffic before recycling storage space… One weekly report on MUSCULAR says the British operators of the site allow the NSA to contribute 100,000 "selectors," or search terms. That is more than twice the number in use in the PRISM program*". Spokesmen for the companies confirmed that this interception was unauthorised by them.

16. It is important to note that the MUSCULAR program involved GCHQ granting access to the NSA to data that it (GCHQ) was holding and permitting it to contribute an extremely large number of selectors. It appears therefore that GCHQ had very limited influence over US access to this data and in respect of the US Government's subsequent use of that data. I understand that controls over US use of UK-intercepted data is an issue in the Application.

17. As the MUSCULAR program was occurring overseas, the government contended it was not regulated by FISA and the FISA Court. Instead, such overseas surveillance is said to be authorised by Executive Order 12333, which provides general authority for the operation of the intelligence agencies under solely Presidential authority, without significant oversight from Congress or the Judiciary.[6] EFF has a primer on Executive Order 12333, which I exhibit hereto at CC2/Pages 61-62[7].

18. Executive Order 12333 was also the likely source for the disclosure, on 4 December 2013, that the NSA was gathering "*nearly 5 billion records a day on the whereabouts of cellphones around the world*"[8]. The Washington Post reported that many Americans'

[6] http://fas.org/irp/offdocs/eo/eo-12333-2008.pdf

[7] https://www.eff.org/deeplinks/2014/06/primer-executive-order-12333-mass-surveillance-starlet

[8] http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html

phones had been caught up in this data sweep, which had been achieved by tapping into the cables that connect mobile networks globally. The vast majority of the records, however, were of non-US persons, including of course, Europeans.

19. Further developments since my first witness statement have included the following:

    19.1. *28 September 2013, New York Times*: the NSA gathered data on the social connections of people around the world, including US and non-US citizens, for the purpose of mapping associations.[9]

    19.2. *19 May 2014, The Intercept*: the NSA had collected the content of *all* cell phone calls made in the Bahamas and four other countries on a rolling 30 day basis. The programs were known as MYSTIC and SOMALGET. This collection, too, was reportedly authorised under Executive Order 12333.[10]

    19.3. *31 May 2014, New York Times*: the NSA was using its surveillance operations to collect "millions" of photographs from online communications each day, 55,000 per day of 'facial recognition' quality, to be used in building a facial recognition database.[11]

    19.4. *30 June 2014, Washington Post*: the FISA Court had permitted spying on a list of 193 countries and other entities such as the World Bank, International Monetary Fund and the European Union.[12]

    19.5. *4 December 2014, The Intercept*: the AURORAGOLD program was disclosed, whereby the NSA and GCHQ obtained technical information on cellphone networks globally, in some cases by subverting encryption standards. The Intercept reported that 70% of global cellphone networks had been hacked in this way.[13]

These and other developments are set out in a timeline document which the Applicants have prepared and I understand will accompany this witness statement.

---

[9] http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html?_r=0
[10] https://firstlook.org/theintercept/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/
[11] http://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html
[12] http://www.washingtonpost.com/world/national-security/court-gave-nsa-broad-leeway-in-surveillance-documents-show/2014/06/30/32b872ec-fae4-11e3-8176-f2c941cf35f1_story.html
[13] https://firstlook.org/theintercept/2014/12/04/nsa-auroragold-hack-cellphones/

Section III: TRANSPARENCY AND LEGAL DEVELOPMENTS

Communications Corporations

20. Since my first witness statement, many more major American internet and telecommunications companies have begun to release "transparency reports" concerning the quantity and type of legal process they receive from American and foreign governments, in response to public concerns[14]. At paragraph 22 of my first witness statement, I referred to the petitions that were filed by several major internet corporations to the FISA Court seeking the lifting of non-disclosure restrictions. In January 2014, the suit was voluntarily dropped and, as a result of the suit, the Justice Department issued a letter setting guidelines for what it would allow companies to publicly report[15]. In summary, six-monthly (instead of annual) reports were permitted, with a six month time lag in reporting, with a more detailed breakdown than previously permitted as to the types of request received, including the number of FISA orders received. Stating the number of accounts affected under each category in bands of 1000 was also permitted. A two year lead-in time was imposed for any new platforms, before the existence of warrants is permitted to be publicised.

21. Notably, Twitter has recently filed a suit against the government seeking to disclose more information than the Government was willing to permit[16].

US Government

22. As I noted in my first statement, the United States government publicly acknowledged the existence of the PRISM and UPSTREAM §702 programs in the wake of the Edward Snowden disclosures. Further government disclosures have followed since then. Since August 2013, the US government has reported on the scope of its domestic national security requests, through the "IC on the Record" website (http://icontherecord.tumblr.com), maintained by the Office of the Director of National Intelligence. Its first Transparency Report, for 2013, was published on 26 June 2014. I exhibit this at Exhibit CC2/Pages 63-68. It shows that pursuant to a single section 702

[14] http://www.theguardian.com/world/2014/feb/03/microsoft-facebook-google-yahoo-fisa-surveillance-requests
[15] http://www.justice.gov/iso/opa/resources/422201412716042240387.pdf http://tmblr.co/ZZQjsq15e967r
[16] http://www.lawfareblog.com/2014/10/twitter-files-lawsuit-against-justice-department-fbi/

FISA "certification", 89,138 persons or groups were targeted for surveillance[17]. However—as the government itself notes—the numbers do not necessarily reflect the actual number of individuals whose communications were intercepted under a given authority, since a "target" may be a group or and individual, and since multiple communications facilities may be intercepted under a single listed authorisation. Moreover, based upon the government's own descriptions of the programs (buttressed by the Washington Post story noted above), the number of people "targeted" is a small fraction of those whose communications or communications records are collected, most of which were analyzed and reviewed by analysts. The figure disclosed is therefore likely to be a tiny fraction of the number of persons whose privacy was affected by the NSA program.

23. At paragraphs 76-81 of my first witness statement I described the concerns regarding the US Government's program of collecting the telephone metadata of all persons in the United States, pursuant to section 215 Patriot Act (which amended section 501 FISA). As a result of Freedom of Information Act lawsuits brought by EFF, on 10 September 2013, the DNI declassified a number of documents regarding the operation of the FISA Court including reports from the NSA to the FISC of a number of compliance incidents involving violations of the FISC's rules governing access to bulk call record metadata. It appears that the violations were so severe and frequent that the FISC considered terminating the program[18]. In 2009 however, the FISA court lifted this requirement and since then has continuously reauthorized the program.

24. On 17 September 2013, the FISA Court released a heavily redacted version of its July ruling approving the renewal of this bulk metadata collection program[19]. While the government unilaterally made some small changes to its use of the information collected under the telephone metadata collection program, as described below in para. 27, the government has not fundamentally changed the collection or the contours of the program. Further 90-day reauthorisations have since followed[20].

[17] http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2013
[18] http://tmblr.co/ZZQjsquh-KGH
[19] http://www.wired.com/2013/09/telcos-metada-orders/
[20] http://www.theguardian.com/world/2014/jun/21/fisa-court-nsa-collection-metadata

25. On 18 November 2013, again as a result of EFF Freedom of Information Act lawsuits, the Director of National Intelligence declassified and released a large amount of documentation relating to US surveillance programs, including two opinions of the FISA Court concerning an Internet metadata collection program authorised under s402 FISA, known as the Pen Register and Trap and Trace (PR/TT) provision.[21] It revealed that the NSA had collected internet metadata from American internet service providers in bulk from 2001 until 2009. The program had been carried out under rolling re-authorisations every 90 days. The program was discontinued in 2011 after a series of serious compliance issues were discovered.

26. On 11 September 2014, the DNI declassified documentation relating to a lawsuit brought in 2007/8 by Yahoo! as a challenge in the FISC to the constitutionality of the Protect America Act— the predecessor statute to the FISA Amendments Act. Yahoo! was required under the PAA to assist the U.S. Government in acquiring foreign intelligence information through the surveillance of foreign surveillance targets[22]. Yahoo! refused to comply with the directives, and the U.S. Government initiated proceedings in the FISC to compel compliance. The law was upheld on appeal, but expired in 2008. It was replaced by the FISA Amendments Act in 2008.

27. Although there have not been any changes to the statutes governing national security surveillance, on January 17, 2014, the President announced a series of reforms for signals intelligence[23]. I exhibit a transcript at Exhibit CC2/Pages 69-74. He announced a review of signals intelligence activities, declassification of additional materials including in relation to the s702 foreign surveillance and s215 telephone metadata programs and certain reforms by presidential decree including an annual review of FISA court opinions for declassification. He also announced his intent to end the s215 bulk metadata program as it currently exists. However now, over a year later, the changes have been minimal. This is because the President has taken the position that any significant changes must be made by Congress. Congress failed to pass a bill containing some of those significant changes.

---

[21] http://america.aljazeera.com/articles/2013/11/19/documents-show-nsaadmitteditoversteppeditsauthorityrepeatedly.html http://tmblr.co/ZZQjsq_oYm8j
[22] http://tmblr.co/ZZQjsq1Qagb8Z
[23] http://icontherecord.tumblr.com/tagged/factsheet

28. During what was a transitional phase, a presidential directive did narrow the searching criteria and required a judicial order for searches, which was subsequently adopted by the FISC, except in emergency cases. He also made it clear that NSA surveillance would be limited to national security and serious crime purposes and not economic advantage, although there is a lack of clarity about how those terms are defined. Finally, he indicated that he had directed the DNI to impose certain limitations on the use of intelligence relating to persons overseas. Those directions resulted in limitations on the duration that personal information is held, the uses to which the information is put, and the circumstances in which it can be disseminated. However, as noted above, these changes do not fundamentally change the nature or scope of the NSA's surveillance programs.

Litigation concerning the surveillance programs

29. A number of courts have considered the constitutionality of the NSA's bulk collection of Americans' phone records. A federal district court in Washington, D.C. declared the program unconstitutional (*Klayman v. Obama*[24]), while courts in New York (*ACLU v. Clapper*[25]), California (*United States* v. *Moalin*), and Idaho (*Smith v. Obama*) upheld the program. All these opinions are currently on appeal, and no appellate court has yet issued a decision to resolve the divergences.

30. At least some criminal defendants are finally being notified if FISA Amendment Act-derived surveillance is relied upon in their prosecutions. From 2008 to 2013, the government failed to provide notice to a single criminal defendant that FAA-derived information had been used in their prosecution. Since the government's change in policy, a few criminal defendants have been notified that FAA surveillance was used (*e.g.*, *United States v. Muhturov*, *United States v. Mohammud*, *United States v. Hasbrajami*, and *United States v. Kahn*). Consequently (and in addition to EFF's longstanding *Jewel v. NSA* litigation), multiple challenges to FAA surveillance are ongoing in federal courts. However, there is still great concern that the government is interpreting its duty to notify very narrowly.

[24] http://scholar.google.com/scholar_case?case=485733189267613105
[25] http://scholar.google.com/scholar_case?case=1687150376533481548

Review by oversight bodies

31. Two governmental reports — issued by independent oversight bodies the Privacy and Civil Liberties Oversight Board ("PCLOB")[26] and a specially convened President's Review Group on Surveillance[27] — both recommended that the NSA's domestic call records metadata collection program should end and both confirmed that it had not significantly aided in any terrorism investigations. Both groups found that the threat to civil liberties posed by the government's bulk collection of call records greatly outweighed any benefit the program provided to national security. The President's Review Group also suggested significant changes to the government's use of Section 702 of FISA.

32. In July 2014, PCLOB issued another report on Section 702 FISA. While PCLOB ultimately took a favorable view of the government's 702 surveillance, there were additional clarifying details in the report that had not been previously disclosed[28]. It described the UPSTREAM collection process in further detail, confirming the massive scale of the initial collection and analysis of communications compared to the relatively small number of people targeted.

33. I do not exhibit the PCLOB and Review Group reports due to their length. However, I can expand upon these further in evidence, including some of the very sharp criticism of their analysis of the 702 programs that exists, if so required.

CONCLUSION

34. In my first witness statement I concluded that the scale of the US surveillance programs was unprecedented and concerning, and that this had not been matched by engagement from the US government. Further disclosures since then have shown that the number and scope of programs is even more concerning than was then thought and these programs are especially concerning with regard to non-US persons, including Europeans. The US government has taken some welcome steps towards greater openness, although many of those came only after EFF and other organizations brought transparency litigation under FOIA.

[26] http://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf
[27] http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf
[28] http://www.pclob.gov/library/702-Report.pdf

35. More importantly, neither substantial changes to the programs nor a wholesale rebalancing towards less intrusion and greater privacy have yet occurred. To the contrary, the US government has now shifted its tactics to claiming that the concern about privacy has gone too far, when in fact almost no significant changes to the scope of collection and analysis (only minimal ones on subsequent use) have occurred.

36. Of particular interest to this Court, very little change to the programs affecting non-US citizens have occurred or are planned. Difficulties through securing accountability through the federal court system and the US Congress also continue.

37. Thus, while EFF and many others in the US continue to pressure the US government to change course and recognize the privacy interests of non-US persons abroad, this Court should not rely on the US courts, Congress or administration to take significant steps to protect Europeans from NSA surveillance or the turning over of that information to GCHQ in the near future.

STATEMENT OF TRUTH

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

SIGNED: .....

Cindy Cohn

DATE: 32 March 2015

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

SECOND 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.deightonpierceglynn.co.uk

On Behalf Of: The Applicants
Name: C. Cohn
Number: Second
Exhibit: CC2
Date: 2 March 2015

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

EXHIBIT CC2

This is Exhibit CC2 to the Second Witness Statement of Cindy Cohn.

The Washington Post

National Security

In NSA-intercepted data, those not targeted far outnumber the foreigners who are

Files provided by Snowden show extent to which ordinary Web users are caught in the net

By Barton Gellman, Julie Tate and Ashkan Soltani July 5, 2014

Ordinary Internet users, American and non-American alike, far outnumber legally targeted foreigners in the communications intercepted by the National Security Agency from U.S. digital networks, according to a four-month investigation by The Washington Post.

Nine of 10 account holders found in a large cache of intercepted conversations, which former NSA contractor Edward Snowden provided in full to The Post, were not the intended surveillance targets but were caught in a net the agency had cast for somebody else.

Many of them were Americans. Nearly half of the surveillance files, a strikingly high proportion, contained names, e-mail addresses or other details that the NSA marked as belonging to U.S. citizens or residents. NSA analysts masked, or "minimized," more than 65,000 such references to protect Americans' privacy, but The Post found nearly 900 additional e-mail addresses, unmasked in the files, that could be strongly linked to U.S. citizens or U.S.residents.

(How 160,000 intercepted conversations led to The Post's latest NSA story)

The surveillance files highlight a policy dilemma that has been aired only abstractly in public. There are discoveries of considerable intelligence value in the intercepted messages — and collateral harm to privacy on a scale that the Obama administration has not been willing to address.

Among the most valuable contents — which The Post will not describe in detail, to avoid interfering with ongoing operations — are fresh revelations about a secret overseas nuclear project, double-dealing by an ostensible ally, a military calamity that befell an unfriendly power, and the identities of aggressive intruders into U.S. computer networks.

Months of tracking communications across more than 50 alias accounts, the files show, led directly to the 2011 capture in Abbottabad of Muhammad Tahir Shahzad, a Pakistan-based bomb builder, and Umar Patek, a suspect in a 2002 terrorist bombing on the Indonesian island of Bali. At the request of CIA officials, The Post is withholding other examples that officials said would compromise ongoing operations.

(Transcript: Q&A with Barton Gellman)

Many other files, described as useless by the analysts but nonetheless retained, have a startlingly intimate, even voyeuristic quality. They tell stories of love and heartbreak, illicit sexual liaisons, mental-health crises, political and religious conversions, financial anxieties and disappointed hopes. The daily lives of more than 10,000 account holders who were not targeted are catalogued and recorded nevertheless.

In order to allow time for analysis and outside reporting, neither Snowden nor The Post has disclosed until now that he obtained and shared the content of intercepted communications. The cache Snowden provided came from domestic NSA operations under the broad authority granted by Congress in 2008 with amendments to the Foreign Intelligence Surveillance Act. FISA content is generally stored in closely controlled data repositories, and for more than a year, senior government officials have depicted it as beyond Snowden's reach.

The Post reviewed roughly 160,000 intercepted e-mail and instant-message conversations, some of them hundreds of pages long, and 7,900 documents taken from more than 11,000 online accounts.

The material spans President Obama's first term, from 2009 to 2012, a period of exponential growth for the NSA's domestic collection.

Taken together, the files offer an unprecedented vantage point on the changes wrought by Section 702 of the FISA amendments, which enabled the NSA to make freer use of methods that for 30 years had required probable cause and a warrant from a judge. One program, code-named PRISM, extracts content stored in user accounts at Yahoo, Microsoft, Facebook, Google and five other leading Internet companies. Another, known inside the NSA as Upstream, intercepts data on the move as it crosses the U.S. junctions of global voice and data networks.

No government oversight body, including the Justice Department, the Foreign Intelligence Surveillance Court, intelligence committees in Congress or the president's Privacy and Civil Liberties Oversight Board, has delved into a comparably large sample of what the NSA actually collects — not only from its targets but also from people who may cross a target's path.

Among the latter are medical records sent from one family member to another, résumés from job hunters and academic transcripts of schoolchildren. In one photo, a young girl in religious dress beams at a camera outside a mosque.

Scores of pictures show infants and toddlers in bathtubs, on swings, sprawled on their backs and kissed by their mothers. In some photos, men show off their physiques. In others, women model lingerie, leaning suggestively into a webcam or striking risque poses in shorts and bikini tops.

"None of the hits that were received were relevant," two Navy cryptologic technicians write in one of many summaries of nonproductive surveillance. "No additional

information," writes a civilian analyst. Another makes fun of a suspected kidnapper, newly arrived in Syria before the current civil war, who begs for employment as a janitor and makes wide-eyed observations about the state of undress displayed by women on local beaches.

By law, the NSA may "target" only foreign nationals located overseas unless it obtains a warrant based on probable cause from a special surveillance court. For collection under PRISM and Upstream rules, analysts must state a reasonable belief that the target has information of value about a foreign government, a terrorist organization or the spread of nonconventional weapons.

Most of the people caught up in those programs are not the targets and would not lawfully qualify as such. "Incidental collection" of third-party communications is inevitable in many forms of surveillance, but in other contexts the U.S. government works harder to limit and discard irrelevant data. In criminal wiretaps, for example, the FBI is supposed to stop listening to a call if a suspect's wife or child is using the phone.

There are many ways to be swept up incidentally in surveillance aimed at a valid foreign target. Some of those in the Snowden archive were monitored because they interacted directly with a target, but others had more-tenuous links.

If a target entered an online chat room, the NSA collected the words and identities of every person who posted there, regardless of subject, as well as every person who simply "lurked," reading passively what other people wrote.

"1 target, 38 others on there," one analyst wrote. She collected data on them all.

In other cases, the NSA designated as its target the Internet protocol, or IP, address of a computer server used by hundreds of people.

The NSA treats all content intercepted incidentally from third parties as permissible to retain, store, search and distribute to its government customers. Raj De, the agency's general counsel, has testified that the NSA does not generally attempt to remove

irrelevant personal content, because it is difficult for one analyst to know what might become relevant to another.

The Obama administration declines to discuss the scale of incidental collection. The NSA, backed by Director of National Intelligence James R. Clapper Jr., has asserted that it is unable to make any estimate, even in classified form, of the number of Americans swept in. It is not obvious why the NSA could not offer at least a partial count, given that its analysts routinely pick out "U.S. persons" and mask their identities, in most cases, before distributing intelligence reports.

If Snowden's sample is representative, the population under scrutiny in the PRISM and Upstream programs is far larger than the government has suggested. In a June 26 "transparency report," the Office of the Director of National Intelligence disclosed that 89,138 people were targets of last year's collection under FISA Section 702. At the 9-to-1 ratio of incidental collection in Snowden's sample, the office's figure would correspond to nearly 900,000 accounts, targeted or not, under surveillance.

'He didn't get this data'

U.S. intelligence officials declined to confirm or deny in general terms the authenticity of the intercepted content provided by Snowden, but they made off-the-record requests to withhold specific details that they said would alert the targets of ongoing surveillance. Some officials, who declined to be quoted by name, described Snowden's handling of the sensitive files as reckless.

In an interview, Snowden said "primary documents" offered the only path to a concrete debate about the costs and benefits of Section 702 surveillance. He did not favor public release of the full archive, he said, but he did not think a reporter could understand the programs "without being able to review some of that surveillance, both the justified and unjustified."

"While people may disagree about where to draw the line on publication, I know that you and The Post have enough sense of civic duty to consult with the government to ensure that the reporting on and handling of this material causes no harm," he said.

In Snowden's view, the PRISM and Upstream programs have "crossed the line of proportionality."

"Even if one could conceivably justify the initial, inadvertent interception of baby pictures and love letters of innocent bystanders," he added, "their continued storage in government databases is both troubling and dangerous. Who knows how that information will be used in the future?"

For close to a year, NSA and other government officials have appeared to deny, in congressional testimony and public statements, that Snowden had any access to the material.

As recently as May, shortly after he retired as NSA director, Gen. Keith Alexander denied that Snowden could have passed FISA content to journalists.

"He didn't get this data," Alexander told a New Yorker reporter. "They didn't touch —"

"The operational data?" the reporter asked.

"They didn't touch the FISA data," Alexander replied. He added, "That database, he didn't have access to."

Robert S. Litt, the general counsel for the Office of the Director of National Intelligence, said in a prepared statement that Alexander and other officials were speaking only about "raw" intelligence, the term for intercepted content that has not yet been evaluated, stamped with classification markings or minimized to mask U.S. identities.

"We have talked about the very strict controls on raw traffic, the training that people

have to have, the technological lockdowns on access," Litt said. "Nothing that you have given us indicates that Snowden was able to circumvent that in any way."

In the interview, Snowden said he did not need to circumvent those controls, because his final position as a contractor for Booz Allen at the NSA's Hawaii operations center gave him "unusually broad, unescorted access to raw SIGINT [signals intelligence] under a special 'Dual Authorities' role," a reference to Section 702 for domestic collection and Executive Order 12333 for collection overseas. Those credentials, he said, allowed him to search stored content — and "task" new collection — without prior approval of his search terms.

"If I had wanted to pull a copy of a judge's or a senator's e-mail, all I had to do was enter that selector into XKEYSCORE," one of the NSA's main query systems, he said.

The NSA has released an e-mail exchange acknowledging that Snowden took the required training classes for access to those systems.

'Minimized U.S. president'

At one level, the NSA shows scrupulous care in protecting the privacy of U.S. nationals and, by policy, those of its four closest intelligence allies — Britain, Australia, Canada and New Zealand.

More than 1,000 distinct "minimization" terms appear in the files, attempting to mask the identities of "possible," "potential" and "probable" U.S. persons, along with the names of U.S. beverage companies, universities, fast-food chains and Web-mail hosts.

Some of them border on the absurd, using titles that could apply to only one man. A "minimized U.S. president-elect" begins to appear in the files in early 2009, and references to the current "minimized U.S. president" appear 1,227 times in the following four years.

Even so, unmasked identities remain in the NSA's files, and the agency's policy is to hold on to "incidentally" collected U.S. content, even if it does not appear to contain foreign intelligence.

In one exchange captured in the files, a young American asks a Pakistani friend in late 2009 what he thinks of the war in Afghanistan. The Pakistani replies that it is a religious struggle against 44 enemy states.

Startled, the American says "they, ah, they arent heavily participating ... its like ... in a football game, the other team is the enemy, not the other teams waterboy and cheerleaders."

"No," the Pakistani shoots back. "The ther teams water boy is also an enemy. it is law of our religion."

"haha, sorry thats kind of funny," the American replies.

When NSA and allied analysts really want to target an account, their concern for U.S. privacy diminishes. The rationales they use to judge foreignness sometimes stretch legal rules or well-known technical facts to the breaking point.

In their classified internal communications, colleagues and supervisors often remind the analysts that PRISM and Upstream collection have a "lower threshold for foreignness 'standard of proof' " than a traditional surveillance warrant from a FISA judge, requiring only a "reasonable belief" and not probable cause.

One analyst rests her claim that a target is foreign on the fact that his e-mails are written in a foreign language, a quality shared by tens of millions of Americans. Others are allowed to presume that anyone on the chat "buddy list" of a known foreign national is also foreign.

In many other cases, analysts seek and obtain approval to treat an account as "foreign" if someone connects to it from a computer address that seems to be overseas. "The best foreignness explanations have the selector being accessed via a foreign IP address," an NSA supervisor instructs an allied analyst in Australia.

Apart from the fact that tens of millions of Americans live and travel overseas, additional millions use simple tools called proxies to redirect their data traffic around the world, for business or pleasure. World Cup fans this month have been using a browser extension called Hola to watch live-streamed games that are unavailable from their own countries. The same trick is routinely used by Americans who want to watch BBC video. The NSA also relies routinely on locations embedded in Yahoo tracking cookies, which are widely regarded by online advertisers as unreliable.

In an ordinary FISA surveillance application, the judge grants a warrant and requires a fresh review of probable cause — and the content of collected surveillance — every 90 days. When renewal fails, NSA and allied analysts sometimes switch to the more lenient standards of PRISM and Upstream.

"These selectors were previously under FISA warrant but the warrants have expired," one analyst writes, requesting that surveillance resume under the looser standards of Section 702. The request was granted.

'I don't like people knowing'

She was 29 and shattered by divorce, converting to Islam in search of comfort and love. He was three years younger, rugged and restless. His parents had fled Kabul and raised him in Australia, but he dreamed of returning to Afghanistan.

One day when she was sick in bed, he brought her tea. Their faith forbade what happened next, and later she recalled it with shame.

"what we did was evil and cursed and may allah swt MOST merciful forgive us for giving in to our nafs [desires]"

Still, a romance grew. They fought. They spoke of marriage. They fought again.

All of this was in the files because, around the same time, he went looking for the Taliban.

He found an e-mail address on its English-language Web site and wrote repeatedly, professing loyalty to the one true faith, offering to "come help my brothers" and join the fight against the unbelievers.

On May 30, 2012, without a word to her, he boarded a plane to begin a journey to Kandahar. He left word that he would not see her again.

If that had been the end of it, there would not be more than 800 pages of anguished correspondence between them in the archives of the NSA and its counterpart, the Australian Signals Directorate.

He had made himself a target. She was the collateral damage, placed under a microscope as she tried to adjust to the loss.

Three weeks after he landed in Kandahar, she found him on Facebook.

"Im putting all my pride aside just to say that i will miss you dearly and your the only person that i really allowed myself to get close to after losing my ex husband, my dad and my brother.. Im glad it was so easy for you to move on and put what we had aside and for me well Im just soo happy i met you. You will always remain in my heart. I know you left for a purpose it hurts like hell sometimes not because Im needy but because i wish i could have been with you."

His replies were cool, then insulting, and gradually became demanding. He would marry her but there were conditions. She must submit to his will, move in with his parents and wait for him in Australia. She must hand him control of her Facebook

account — he did not approve of the photos posted there.

She refused. He insisted:

"look in islam husband doesnt touch girl financial earnigs unless she agrees but as far as privacy goes there is no room....i need to have all ur details everything u do its what im supposed to know that will guide u whether its right or wrong got it"

Later, she came to understand the irony of her reply:

"I don't like people knowing my private life."

Months of negotiations followed, with each of them declaring an end to the romance a dozen times or more. He claimed he had found someone else and planned to marry that day, then admitted it was a lie. She responded:

"No more games. You come home. You won't last with an afghan girl."

She begged him to give up his dangerous path. Finally, in September, she broke off contact for good, informing him that she was engaged to another man.

"When you come back they will send you to jail," she warned.

They almost did.

In interviews with The Post, conducted by telephone and Facebook, she said he flew home to Australia last summer, after failing to find members of the Taliban who would take him seriously. Australian National Police met him at the airport and questioned him in custody. They questioned her, too, politely, in her home. They showed her transcripts of their failed romance. When a Post reporter called, she already knew what the two governments had collected about her.

Eventually, she said, Australian authorities decided not to charge her failed suitor with a crime. Police spokeswoman Emilie Lovatt declined to comment on the case.

Looking back, the young woman said she understands why her intimate correspondence was recorded and parsed by men and women she did not know.

"Do I feel violated?" she asked. "Yes. I'm not against the fact that my privacy was violated in this instance, because he was stupid. He wasn't thinking straight. I don't agree with what he was doing."

What she does not understand, she said, is why after all this time, with the case long closed and her own job with the Australian government secure, the NSA does not discard what it no longer needs.

Jennifer Jenkins and Carol D. Leonnig contributed to this report.

Barton Gellman writes for the national staff. He has contributed to three Pulitzer Prizes for The Washington Post, most recently the 2014 Pulitzer Prize for Public Service.

EXHIBIT A

PROCEDURES USED BY THE NATIONAL SECURITY AGENCY FOR TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED

(S) These procedures address: (I) the manner in which the National Security Agency/Central Security Service (NSA) will determine that a person targeted under section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended ("the Act"), is a non-United States person reasonably believed to be located outside the United States ("foreignness determination"); (II) the post-targeting analysis done by NSA to ensure that the targeting of such person does not intentionally target a person known at the time of acquisition to be located in the United States and does not result in the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States; (III) the documentation of NSA's foreignness determination; (IV) compliance and oversight; and (V) departures from these procedures.

I. (U) DETERMINATION OF WHETHER THE ACQUISITION TARGETS NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES

(S) NSA determines whether a person is a non-United States person reasonably believed to be outside the United States in light of the totality of the circumstances based on the information available with respect to that person, including information concerning the communications facility or facilities used by that person.

(S) NSA analysts examine the following three categories of information, as appropriate under the circumstances, to make the above determination: (1) they examine the lead information they have received regarding the potential target or the facility that has generated interest in conducting surveillance to determine what that lead information discloses about the person's location; (2) they conduct research in NSA databases, available reports and collateral information (i.e., information to which NSA has access but did not originate, such as reports from other agencies and publicly available information) to determine whether NSA knows the location of the person, or knows information that would provide evidence concerning that location; and (3) they conduct technical analyses of the facility or facilities to determine or verify information about the person's location. NSA may use information from any one or a combination of these categories of information in evaluating the totality of the circumstances to determine that the potential target is located outside the United States.

(TS//SI) In addition, in those cases where NSA seeks to acquire communications about the target that are not to or from the target, NSA will either employ an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

overseas, or it will target Internet links that terminate in a foreign country. In either event, NSA will direct surveillance at a party to the communication reasonably believed to be outside the United States.

(S) Lead Information

(S) When NSA proposes to direct surveillance at a target, it does so because NSA has already learned something about the target or the facility or facilities the target uses to communicate. Accordingly, NSA will examine the lead information to determine what it reveals about the physical location of the target, including the location of the facility or facilities being used by the potential target.

(S) The following are examples of the types of lead information that NSA may examine:

a) Has the target stated that he is located outside the United States? For example, has NSA or another intelligence agency collected a statement or statements made by the target indicating that he is located outside the United States?

b) Has a human intelligence source or other source of lead information indicated that the target is located outside the United States?

c) Does the lead information provided by an intelligence or law enforcement agency of the United States government or an intelligence or law enforcement service of a foreign government indicate that the target is located outside the United States?

d) Was the lead information about the target found on a hard drive or other medium that was seized in a foreign country?

e) With whom has the target had direct contact, and what do we know about the location of such persons? For example, if lead information indicates the target is in direct contact with several members of a foreign-based terrorist organization or foreign-based political organization who themselves are located overseas, that may suggest, depending on the totality of the circumstances, that the target is also located overseas.

(S) Information NSA Has About the Target's Location and/or Facility or Facilities Used by the Target

(S) NSA may also review information in its databases, including repositories of information collected by NSA and by other intelligence agencies, as well as publicly available information, to determine if the person's location, or information providing evidence about the person's location, is already known. The NSA databases that would be used for this purpose contain information culled from signals intelligence, human intelligence, law enforcement information, and other sources. For example, NSA databases may include a report produced by the Central Intelligence Agency (CIA) with the fact that a known terrorist is using a telephone with a particular number, or detailed information on worldwide telephony numbering plans for wire and wireless telephone systems.

(S) NSA Technical Analysis of the Facility

(S) NSA may also apply technical analysis concerning the facility from which it intends to acquire foreign intelligence information to assist it in making determinations concerning the location of the person at whom NSA intends to direct surveillance. For example, NSA may examine the following types of information:

(S) For telephone numbers:

a) Identify the country code of the telephone number, and determine what it indicates about the person's location.

b) Review commercially available and NSA telephone numbering databases for indications of the type of telephone being used (e.g. landline, wireless mobile, satellite, etc.), information that may provide an understanding of the location of the target.

(S) For electronic communications accounts/addresses/identifiers:

Review NSA content repositories and Internet communications data repositories (which contain, among other things, Internet communications metadata) for previous Internet activity. This information may contain network layer (e.g., Internet Protocol addresses) or machine identifier (e.g., Media Access Control addresses) information, which NSA compares to information contained in NSA's communication network databases and commercially available Internet Protocol address registration information in order to determine the location of the target.

(S) Assessment of the Non-United States Person Status of the Target

(S) In many cases, the information that NSA examines in order to determine whether a target is reasonably believed to be located outside the United States may also bear upon the non-United States person status of that target. For example, lead information provided by an intelligence or law enforcement service of a foreign government may indicate not only that the target is located in a foreign country, but that the target is a citizen of that or another foreign country. Similarly, information contained in NSA databases, including repositories of information collected by NSA and by other intelligence agencies, may indicate that the target is a non-United States person.

(S) Furthermore, in order to prevent the inadvertent targeting of a United States person, NSA maintains records of telephone numbers and electronic communications accounts/addresses/ identifiers that NSA has reason to believe are being used by United States persons. Prior to targeting, a particular telephone number or electronic communications account/address/identifier will be compared against those records in order to ascertain whether NSA has reason to believe that telephone number or electronic communications account/address/identifier is being used by a United States person.

(S) In the absence of specific information regarding whether a target is a United States person, a person reasonably believed to be located outside the United States or whose location is not known will be presumed to be a non-United States person unless such person can be positively identified as a United States person, or the nature or circumstances of the person's communications give rise to a reasonable belief that such person is a United States person.

(S) Assessment of the Foreign Intelligence Purpose of the Targeting

(S) In assessing whether the target possesses and/or is likely to communicate foreign intelligence information concerning a foreign power or foreign territory, NSA considers, among other things, the following factors:

a. With respect to telephone communications:

- Information indicates that the telephone number has been used to communicate directly with another telephone number reasonably believed by the U.S. Intelligence Community to be used by an individual associated with a foreign power or foreign territory;

- Information indicates that a user of the telephone number has communicated directly with an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;

- Information indicates that the telephone number is listed in the telephone directory of a telephone used by an individual associated with a foreign power or foreign territory;

- Information indicates that the telephone number has been transmitted during a telephone call or other communication with an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;

- Publicly available sources of information (e.g., telephone listings) match the telephone number to an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;

- Information contained in various NSA-maintained knowledge databases containing foreign intelligence information acquired by any lawful means, such as electronic surveillance, physical search, or the use of a pen register and trap or trace device, or other information, reveals that the telephone number has been previously used by an individual associated with a foreign power or foreign territory;[1] or

[1] (TS//SI//NF) The NSA knowledge databases that would be used to satisfy this factor contain fused intelligence information concerning international terrorism culled from signals intelligence, human intelligence, law enforcement information, and other sources. The information compiled in these databases is information that assists the signals intelligence system in effecting collection on intelligence targets. For example, a report produced by the CIA may include the fact that a known terrorist is using a telephone with a particular number. NSA would include that information in its knowledge databases.

- Information made available to NSA analysts as a result of processing telephony metadata records acquired by any lawful means, such as electronic surveillance, physical search, or the use of a pen register or trap and trace device, or other information, reveals that the telephone number is used by an individual associated with a foreign power or foreign territory.

b. With respect to Internet communications:

- Information indicates that the electronic communications account/address/identifier has been used to communicate directly with an electronic communications account/address/identifier reasonably believed by the U.S. Intelligence Community to be used by an individual associated with a foreign power or foreign territory;

- Information indicates that a user of the electronic communications account/address/identifier has communicated directly with an individual reasonably believed to be associated with a foreign power or foreign territory;

- Information indicates that the electronic communications account/address/identifier is included in the "buddy list" or address book of an electronic communications account/address/identifier reasonably believed by the U.S. Intelligence Community to be used by an individual associated with a foreign power or foreign territory;

- Information indicates that the electronic communications account/address/identifier has been transmitted during a telephone call or other communication with an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;

- Public Internet postings match the electronic communications account/address/identifier to an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;

- Information contained in various NSA-maintained knowledge databases of foreign intelligence information acquired by any lawful means, such as electronic surveillance, physical search, the use of a pen register or trap and trace device, or other information, reveals that electronic communications account/address/identifier has been previously used by an individual associated with a foreign power or foreign territory;

- Information made available to NSA analysts as a result of processing metadata records acquired by any lawful means, such as electronic surveillance, physical search, or the use of a pen register or trap and trace device, or other information, reveals that the electronic communications account/address/identifier is used by an individual associated with a foreign power or foreign territory; or

- Information indicates that Internet Protocol ranges and/or specific electronic identifiers or signatures (e.g., specific types of cryptology or steganography) are used almost exclusively by individuals associated with a foreign power or foreign territory,

or are extensively used by individuals associated with a foreign power or foreign territory.

II. (S) POST-TARGETING ANALYSIS BY NSA

(S//SI) After a person has been targeted for acquisition by NSA, NSA will conduct post-targeting analysis. Such analysis is designed to detect those occasions when a person who when targeted was reasonably believed to be located outside the United States has since entered the United States, and will enable NSA to take steps to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States, or the intentional targeting of a person who is inside the United States. Such analysis may include:

For telephone numbers:

- Routinely comparing telephone numbers tasked pursuant to these procedures against information that has been incidentally collected from the Global System for Mobiles (GSM) Home Location Registers (HLR). These registers receive updates whenever a GSM phone moves into a new service area. Analysis of this HLR information provides a primary indicator of a foreign user of a mobile telephone entering the United States.

- NSA analysts may analyze content for indications that a foreign target has entered or intends to enter the United States. Such content analysis will be conducted according to analytic and intelligence requirements and priorities.

For electronic communications accounts/addresses/identifiers:

- Routinely checking all electronic communications accounts/addresses/identifiers tasked pursuant to these procedures against available databases that contain Internet communications data (including metadata) to determine if an electronic communications account/address/identifier was accessed from overseas. Such databases contain communications contact information and summaries of communications activity from NSA signals intelligence collection. The foreign access determination is made based on comparing the Internet Protocol address associated with the account activity to other information NSA possesses about geographical area(s) serviced by particular Internet Protocol addresses. If the IP address associated with the target activity is identified as a U.S.-based network gateway (e.g., a Hotmail server) or a private Internet Protocol address, then NSA analysts will be required to perform additional research to determine if the access was in a foreign country using additional criteria such as machine identifier or case notation (NSA circuit identifier) of a communications link known to be foreign. Such databases normally maintain information about such activity for a 12-month period. This data will be used in an attempt to rule out false positives from U.S.-based network gateways. If the account access is determined to be from a U.S.-based machine, further analytic checks will be performed using content collection to determine if the target has moved into the United States.

- Routinely comparing electronic communications accounts/addresses/identifiers tasked pursuant to these procedures against a list of electronic communications accounts/ addresses/identifiers already identified by NSA as being accessed from inside the United States. This will help ensure that no target has been recognized to be located in the United States.

- NSA analysts may analyze content for indications that a target has entered or intends to enter the United States. Such content analysis will be conducted according to analytic and intelligence requirements and priorities.

(S) If NSA determines that a target has entered the United States, it will follow the procedures set forth in section IV of this document, including the termination of the acquisition from the target without delay. In cases where NSA cannot resolve an apparent conflict between information indicating that the target has entered the United States and information indicating that the target remains located outside the United States, NSA will presume that the target has entered the United States and will terminate the acquisition from that target. If at a later time NSA determines that the target is in fact located outside the United States, NSA may re-initiate the acquisition in accordance with these procedures.

(S) If NSA determines that a target who at the time of targeting was believed to be a non-United States person was in fact a United States person, it will follow the procedures set forth in section IV of this document, including the termination of the acquisition from the target without delay.

III. (U) DOCUMENTATION

(S) Analysts who request tasking will document in the tasking database a citation or citations to the information that led them to reasonably believe that a targeted person is located outside the United States. Before tasking is approved, the database entry for that tasking will be reviewed in order to verify that the database entry contains the necessary citations.

(S) A citation is a reference that identifies the source of the information, such as a report number or communications intercept identifier, which NSA will maintain. The citation will enable those responsible for conducting oversight to locate and review the information that led NSA analysts to conclude that a target is reasonably believed to be located outside the United States.

(S) Analysts also will identify the foreign power or foreign territory about which they expect to obtain foreign intelligence information pursuant to the proposed targeting.

IV. (U) OVERSIGHT AND COMPLIANCE

(S) NSA's Signals Intelligence Directorate (SID) Oversight and Compliance, with NSA's Office of General Counsel (OGC), will develop and deliver training regarding the applicable procedures to ensure intelligence personnel responsible for approving the targeting of persons under these procedures, as well as analysts with access to the acquired foreign intelligence information understand their responsibilities and the procedures that apply to this acquisition. SID Oversight and Compliance has established processes for ensuring that raw traffic is labeled and stored only in authorized repositories, and is accessible only to those who have had the proper training. SID

Oversight and Compliance will conduct ongoing oversight activities and will make any necessary reports, including those relating to incidents of noncompliance, to the NSA Inspector General and OGC, in accordance with its NSA charter. SID Oversight and Compliance will also ensure that necessary corrective actions are taken to address any identified deficiencies. To that end, SID Oversight and Compliance will conduct periodic spot checks of targeting decisions and intelligence disseminations to ensure compliance with established procedures, and conduct periodic spot checks of queries in data repositories.

(S) The Department of Justice (DOJ) and the Office of the Director of National Intelligence (ODNI) will conduct oversight of NSA's exercise of the authority under section 702 of the Act, which will include periodic reviews by DOJ and ODNI personnel to evaluate the implementation of the procedures. Such reviews will occur at least once every sixty days.

(S) NSA will report to DOJ, to the ODNI Office of General Counsel, and to the ODNI Civil Liberties Protection Officer any incidents of noncompliance with these procedures by NSA personnel that result in the intentional targeting of a person reasonably believed to be located in the United States, the intentional targeting of a United States person, or the intentional acquisition of any communication in which the sender and all intended recipients are known at the time of acquisition to be located within the United States. NSA will provide such reports within five business days of learning of the incident. Any information acquired by intentionally targeting a United States person or a person not reasonably believed to be outside the United States at the time of such targeting will be purged from NSA databases.

(S) NSA will report to DOJ through the Deputy Assistant Attorney General in the National Security Division with responsibility for intelligence operations and oversight, to the ODNI Office of General Counsel, and to the ODNI Civil Liberties Protection Officer, any incidents of noncompliance (including overcollection) by any electronic communication service provider to whom the Attorney General and Director of National Intelligence issued a directive under section 702. Such report will be made within five business days after determining that the electronic communication service provider has not complied or does not intend to comply with a directive.

(S) In the event that NSA concludes that a person is reasonably believed to be located outside the United States and after targeting this person learns that the person is inside the United States, or if NSA concludes that a person who at the time of targeting was believed to be a non-United States person was in fact a United States person, it will take the following steps:

1) Terminate the acquisition without delay and determine whether to seek a Court order under another section of the Act. If NSA inadvertently acquires a communication sent to or from the target while the target is or was located inside the United States, including any communication where the sender and all intended recipients are reasonably believed to be located inside the United States at the time of acquisition, such communication will be treated in accordance with the applicable minimization procedures.

2) Report the incident to DOJ through the Deputy Assistant Attorney General in the National Security Division with responsibility for intelligence operations and oversight, to the ODNI Office of General Counsel, and to the ODNI Civil Liberties Protection Officer within five business days.

V. (U) DEPARTURE FROM PROCEDURES

(S) If, in order to protect against an immediate threat to the national security, NSA determines that it must take action, on a temporary basis, in apparent departure from these procedures and that it is not feasible to obtain a timely modification of these procedures from the Attorney General and Director of National Intelligence, NSA may take such action and will report that activity promptly to DOJ through the Deputy Assistant Attorney General in the National Security Division with responsibility for intelligence operations and oversight, to the ODNI Office of General Counsel, and to the ODNI Civil Liberties Protection Officer. Under such circumstances, the Government will continue to adhere to all of the statutory limitations set forth in subsection 702(b) of the Act.

7-28-09
Date

Eric H. Holder, Jr.
Attorney General of the United States

SPIEGEL ONLINE
06/18/2014 04:20 PM

New NSA Revelations

Inside Snowden's Germany File

By SPIEGEL Staff

An analysis of secret documents leaked by Edward Snowden demonstrates that the NSA is more active in Germany than anywhere else in Europe -- and that data collected here may have helped kill suspected terrorists.

Just before Christmas 2005, an unexpected event disrupted the work of American spies in the south-central German city of Wiesbaden. During the installation of a fiber-optic cable near the Rhine River, local workers encountered a suspicious metal object, possibly an undetonated World War II explosive. It was certainly possible: Adolf Hitler's military had once maintained a tank repair yard in the Wiesbaden neighborhood of Mainz-Kastel.

The Americans -- who maintained what was officially known as a "Storage Station" on Ludwig Wolker Street -- prepared an evacuation plan. And on Jan. 24, 2006, analysts with the National Security Agency (NSA) cleared out their offices, cutting off the intelligence agency's access to important European data streams for an entire day, a painfully long time. The all-clear only came that night: The potential ordinance turned out to be nothing more than a pile of junk.

Residents in Mainz-Kastel knew nothing of the incident.

Of course, everybody living there knows of the 20-hectare (49-acre) US army compound. A beige wall topped with barbed wire protects the site from the outside world; a sign outside warns, "Beware, Firearms in Use!"

Americans in uniform have been part of the cityscape in Wiesbaden for decades, and local businesses have learned to cater to their customers from abroad. Used-car dealerships post their prices in dollars and many Americans are regulars at the local brewery. "It is a peaceful coexistence," says Christa Gabriel, head of the Mainz-Kastel district council.

But until now, almost nobody in Wiesbaden knew that Building 4009 of the "Storage Station" houses one of the NSA's most important European data collection centers. Its official name is the European Technical Center (ETC), and, as documents from the archive of whistleblower Edward Snowden show, it has been expanded in recent years. From an American perspective, the program to improve the center -- which was known by the strange code name "GODLIKELESION" -- was badly needed. In early 2010, for example, the NSA branch office lost power 150 times within the space just a few months -- a serious handicap for a service that strives to monitor all of the world's data traffic.

On Sept. 19, 2011, the Americans celebrated the reopening of the refurbished ETC, and since then, the building has been the NSA's "primary communications hub" in Europe. From here, a Snowden document outlines, huge amounts of data are intercepted and forwarded to "NSAers, warfighters and foreign partners in Europe, Africa and the Middle East." The hub, the document notes, ensures the reliable transfer of data for "the foreseeable future."

Soon the NSA will have an even more powerful and modern facility at their disposal: Just five kilometers away, in the Clay Kaserne, a US military complex located in the Erbenheim district of Wiesbaden, the "Consolidated Intelligence Center" is under construction. It will house data-monitoring specialists from Mainz-Kastel. The project in southern Hesse comes with a price tag of $124 million (€91 million). When finished, the US government will be even better equipped to satisfy its vast hunger for data.

One year after Edward Snowden made the breadth of the NSA's global data monitoring public, much remains unknown about the full scope of the intelligence service's activities in Germany. We know that the Americans monitored the mobile phone of German Chancellor Angela Merkel and

we know that there are listening posts in the US Embassy in Berlin and in the Consulate General in Frankfurt.

But much remains in the dark. The German government has sent lists of questions to the US government on several occasions, and a parliamentary investigative committee has begun looking into the subject in Berlin. Furthermore, Germany's chief public prosecutor has initiated an investigation into the NSA -- albeit one currently limited to its monitoring of the chancellor's cell phone and not the broader allegation that it spied on the communications of the German public. Neither the government nor German lawmakers nor prosecutors believe they will receive answers from officials in the United States.

German Left Party politician Jan Korte recently asked just how much the German government knows about American spying activities in Germany. The answer: Nothing. The NSA's promise to send a package including all relevant documents to re-establish transparency between the two governments has been quietly forgotten by the Americans.

In response, SPIEGEL has again reviewed the Snowden documents relating to Germany and compiled a Germany File of original documents pertaining to the NSA's activities in the country that are now available for download here. SPIEGEL has reported on the contents of some of the documents over the course of the past year. The content of others is now being written about for the first time. Some passages of the documents have been redacted in order to remove sensitive information like the names of NSA employees or those of the German foreign intelligence service, the Bundesnachrichtendienst (BND). This week's reports are also based on documents and information from other sources.

An Omnipotent American Authority

The German public has a right to know exactly what the NSA is doing in Germany, and should be given the ability to draw its own conclusions about the extent of the US intelligence agency's activities in the country and the scope of its cooperation with German agencies when it comes to, for example, the monitoring of fiber-optic cables.

The German archive provides the basis for a critical discussion on the necessity and limits of secret service work as well as on the protection of privacy in the age of digital communication. The documents complement the debate over a trans-Atlantic relationship that has been severely damaged by the NSA affair.

They paint a picture of an all-powerful American intelligence agency that has developed an increasingly intimate relationship with Germany over the past 13 years while massively expanding its presence. No other country in Europe plays host to a secret NSA surveillance architecture comparable to the one in Germany. It is a web of sites defined as much by a thirst for total control as by the desire for security. In 2007, the NSA claimed to have at least a dozen active collection sites in Germany.

The documents indicate that the NSA uses its German sites to search for a potential target by analyzing a "Pattern of Life," in the words of one Snowden file. And one classified report suggests that information collected in Germany is used for the "capture or kill" of alleged terrorists.

According to Paragraph 99 of Germany's criminal code, spying is illegal on German territory, yet German officials would seem to know next to nothing about the NSA's activity in their country. For quite some time, it appears, they didn't even want to know. It wasn't until Snowden went public with his knowledge that the German government became active.

On June 11, August 26 and October 24 of last year, Berlin sent a catalogue of questions to the US government. During a visit to NSA headquarters at Fort Meade, Maryland at the beginning of November, German intelligence heads Gerhard Schindler (of the BND) and Hans-Georg Maassen (of the domestic intelligence agency, known as the Office for the Protection of the Constitution or BfV) asked the most important questions in person and, for good measure, handed over a written list. No answers have been forthcoming. This leaves the Snowden documents as the best source for describing how the NSA has turned Germany into its most important base in Europe in the wake of the terrorist attacks of Sept. 11, 2001.

The NSA's European Headquarters

On March 10, 2004, two US generals -- Richard J. Quirk III of the NSA and John Kimmons, who was the US Army's deputy chief of staff for intelligence -- finalized an agreement to establish an operations center in Germany, the European Security Center (ESC), to be located on US Army property in the town of Griesheim near Darmstadt, Germany. That center is now the NSA's most important listening station in Europe.

The NSA had already dispatched an initial team to southern Germany in early 2003. The agency stationed a half-dozen analysts at the its European headquarters in Stuttgart's Vaihingen neighborhood, where their work focused largely on North Africa. The analysts' aims, according to internal documents, included providing support to African governments in securing borders and ensuring that they didn't offer safe havens to terrorist organizations or their accomplices.

The work quickly bore fruit. It became increasingly easy to track the movements of suspicious persons in Mali, Mauritania and Algeria through the surveillance of satellite telephones. NSA workers passed information on to the US military's European Command, with some also being shared with individual governments in Africa. A US government document states that the intelligence insights have "been responsible for the capture or kill of over 40 terrorists and has helped achieve GWOT (Global War on Terror) and regional policy successes in Africa."

Is Germany an NSA Beachhead?

The documents in Snowden's archive raise the question of whether Germany has become a beachhead for America's deadly operations against suspected terrorists -- and whether the CIA and the American military use data collected in Germany in the deployment of its combat drones. When asked about this by SPIEGEL, the NSA declined to respond.

The operations of the NSA's analysts in Stuttgart were so successful that the intelligence agency quickly moved to expand its presence. In 2004, the Americans obtained approximately 1,000 square meters (10,750 square feet) of office space in Griesheim to host 59 workers who monitored communications in an effort to "optimize support to Theater operations" of the US Armed Forces. Ten years later, the center, although largely used by the military, has become the NSA's most important outpost in Europe -- with a mandate that goes far beyond providing support for the US military.

In 2011, around 240 intelligence service analysts were working at the Griesheim facility, known as the Dagger Complex. It was a "diverse mix of military service members, Department of the Army civilians, NSA civilians, and contractors," an internal document states. They were responsible for both collecting and analyzing international communication streams. One member of the NSA pointed out proudly that they were responsible for every step in the process: collection, processing, analyzing and distribution.

In May 2011, the installation was renamed the European Center for Cryptology (ECC) and the NSA integrated its Threat Operations Center, responsible for early danger identification, into the site. A total of 26 reconnaissance missions are managed from the Griesheim complex, which has since become the center of the "largest Analysis and Production activity in Europe," with satellite stations in Mons, Belgium, and in Great Britain. Internal documents indicate that the ECC is the operative intelligence arm of the NSA's European leadership in Stuttgart.

Targets in Africa, Targets in Europe

Much of what happens in Griesheim is classic intelligence work and threat identification, but a presentation dating from 2012 suggests that European data streams are also monitored on a broad scale. One internal document states there are targets in Africa as well as targets in Europe. The reason being that "most terrorists stop thru Europe." For reconnaissance, the document mentions, the ECC relies on its own intelligence gathering as well as data and assistance from Britain's Government Communications Headquarters (GCHQ) intelligence service.

The latter is likely a reference to the Tempora program, located in the British town of Bude, which collects all Internet data passing through several major fiber-optic cables. GCHQ, working together with the NSA, saves the data that travels through these major European network connections for at least three days. The ECC claims to have access to at least part of the GCHQ data.

NSA staff in Griesheim use the most modern equipment available for the analysis of the data streams, using programs like XKeyscore, which allows for the deep penetration of Internet traffic. Xkeyscore's sheer power even awakened the interest of Germany's BND foreign intelligence service as well as that of the Federal Office for the Protection of the Constitution, which is responsible for monitoring extremists and possible terrorists within Germany.

An internal NSA report suggests that XKeyscore was being used at Griesheim not only to collect metadata -- e.g. the who, what, where, with whom and at what time -- but also the content of actual communications. "Raw content" is saved for a period of between "3 days to a couple of weeks," an ECC slide states. The metadata are stored for more than 90 days. The document states that XKeyscore also makes "complex analytics like 'Pattern of Life'" possible.

The NSA said in a statement that XKeyscore is an element of its foreign intelligence gathering activities, but it was using the program lawfully and that it allows the agency to help "defend the nation and protect US and allied troops abroad." The statement said it engages in "extensive, close consultations" with the German government. In a statement provided to SPIEGEL, NSA officials pointed to a policy directive Barack Obama issued in January in which the US president affirmed that all persons, regardless of nationality, have legitimate privacy interests, and that privacy and civil liberties "shall be integral considerations in the planning of US signals intelligence activities."

The statement reveals the significant gap between Germany's understanding of what surveillance means and that of the Americans. In overseas operations, the NSA does not consider searching through emails to be surveillance as long as they are only stored temporarily. It is only considered to be a deeper encroachment on privacy when this data is transferred to the agency's databases and saved for a longer period of time. The US doesn't see it as a contradiction when Obama ensures that people won't be spied upon, even as the NSA continues monitoring email traffic. The NSA did not respond to SPIEGEL's more detailed questions about the agency's outposts in Germany.

'The Endangered Habitat of the NSA Spies'

The bustling activity inside the Dagger Complex listening station at Griesheim stands in stark contrast to its outward appearance. Only a few buildings can be recognized above ground, secured by two fences and a gate made of steel girders and topped by barbed wire.

Activist Daniel Bangart would love to see what is on the other side of that fence. He's rattled the fence a number of times over the past year, but so far no one has let him in. Instead, he's often been visited by police.

When Bangert first began inviting people to take a "walk" at Griesheim to "explore together the endangered habitat of the NSA spies," he intended it as a kind of subversive satirical act. But with each new revelation from the Snowden archive, the 29-year-old has taken the issue more seriously. These days, the heating engineer -- who often wears a T-shirt emblazoned with "Team Edward" -- and a small group of campaigners regularly attempt to provoke employees at the Dagger Complex. He has developed his own method of counter-espionage: He writes down the license plate numbers of suspected spies from Wiesbaden and Stuttgart.

At one point, the anti-surveillance activist even tried to initiate a dialogue with a few of the Americans. At a street fair in Griesheim, he convinced one to join him for a beer, but the man only answered Bangert's questions with queries of his own. Bangert says another American told him: "What is your problem? We are watching you!"

Spying as They Please

It's possible Bangert has also attracted the attention of another NSA site, located in the US Consulate General in Frankfurt, not far from Griesheim. The "Special Collection Service" (SCS) is a listening station that German public prosecutors have taken a particular interest in since announcing earlier this month that it was launching an investigation into the spying on Angela Merkel's mobile phone. The trail leads from the Chancellery in Berlin via the US Embassy next to the Brandenburg Gate and continues all the way to Laurel, Maryland, north of Washington DC.

That's where the SCS is headquartered. The service is operated together by the NSA and the CIA and has agents spread out across the globe. They are the eyes and ears of the US and, as one internal document notes, establish a "Home field advantage in adversary's space."

The SCS is like a two-parent household, says Ron Moultrie, formerly the service's vice president. "We must be mindful of both 'parents'." Every two years, leadership is swapped between the NSA and the CIA. The SCS, says Moultrie, is "truly a hybrid." It is divided into four departments, including the "Mission Support Office" and the "Field Operations Office," which is made up of a Special Operations unit and a center for signal development. In Laurel, according to internal documents, the NSA has established a relay station for communications intercepted overseas and a site for training.

Employees are stationed in US embassies and consulates in crisis regions, but are also active in countries that are considered neutral, like Austria. The agents are protected by diplomatic accreditation, even though their job isn't covered by the international agreements guaranteeing diplomatic immunity: They spy pretty much as they please. For many years, SCS agents claimed to be working for the ominous-sounding "Defense Communications Support Group." Sometimes, they said they worked for something called the "Defense Information Systems Agency."

Spying Stations, from Athens the Zagreb

According to an internal document from 2011, information related to the SCS and the sites it maintains was to be kept classified for at least 75 years. It argued that if the agency's activities were ever revealed, it would hamper the "effectiveness of intelligence methods currently in use" and result in "serious harm" to relations between the US and foreign governments.

In 1979, there were just over 40 such SCS branch offices. During the chilliest days of the Cold War, the number reached a high point of 88 only to drop significantly after the fall of the Berlin Wall and the collapse of communism in Eastern Europe. But following the Sept. 11, 2001 terror attacks, the government established additional sites, bringing the number of SCS spy stations around the world up to a total of around 80 today. The documents indicate that the SCS maintains two sites in Germany: in the US Consulate General in Frankfurt and the US Embassy in Berlin, just a few hundred meters away from the Chancellery.

The German agencies responsible for defending against and pursuing espionage -- the Office for the Protection of the Constitution and the office of the chief federal prosecutor -- are particularly interested in the technology deployed by the SCS. The database entry relating to Merkel's cell phone, which SPIEGEL first reported on in October 2013, shows that the SCS was responsible for its surveillance.

According to an internal presentation about the work done by the SCS, equipment includes an antenna rotator known as "Einstein," a database for analysis of microwaves called "Interquake" and a program called "Sciatica" that allows for the collection of signals transmitted in gigahertz frequencies. A program called "Birdwatcher," which intercepts encrypted signals and prepares them for analysis, can be remotely controlled from the SCS headquarters in Maryland. The tool allows the NSA to identify protected "Virtual Private Networks" or VPNs that might be of interest. VPNs are used by many companies and embassies for internal communication.

200 American Intelligence Workers in Germany

Following the revelations that Merkel's mobile phone had been monitored, Hans-Georg Maassen of the domestic intelligence agency BfV, turned to US Ambassador to Germany John Emerson to learn more about the technology and the people behind it. Maassen also wanted to know what private contractors the NSA was working with in Germany. When Emerson said during a visit to the Chancellery that he assumed the questions had been straightened out, Maassen countered, in writing, that they remained pertinent.

Maassen says he received a "satisfactory" answer from Emerson about intelligence employees. But that could be because the US government has officially accredited a number of the intelligence workers it has stationed in Germany. SPIEGEL research indicates more than 200 Americans are registered as diplomats in Germany. There are also employees with private firms who are contracted by the NSA but are not officially accredited.

The list of questions the German government sent to the US Embassy makes it clear that German intelligence badly needs help. "Are there Special Collection Services in Germany?" reads one question. "Do you conduct surveillance in Germany?" And: "Is this reconnaissance targeted against German interests? " There are many questions, but no answers.

Ultimately, Maassen will have to explain to the parliamentary investigative committee what he has learned about US spying in Germany and how he intends to fulfill his legally mandated task of preventing espionage. The explanation provided by the BfV thus far -- that it is uncertain whether the chancellor was spied on from the US Embassy in Berlin or remotely from the headquarters in Maryland, making it unclear whether German anti-espionage officials should get involved -- is certainly an odd one. Germany's domestic intelligence agency is responsible for every act of espionage targeting the country, no matter where it originates. Cyber-attacks from China are also viewed by the BfV as espionage, even if they are launched from Shanghai.

The order to monitor the chancellor was issued by the department S2C32, the NSA unit responsible for Europe. In 2009, Merkel was included in a list of 122 heads of state and government being spied on by the NSA. The NSA collects all citations relating to a specific person, including the different ways of referring to them, in a database called "Nymrod."

The NSA introduced Nymrod in January 2008 and the entries refer to a kind of register of "intelligence reports from NSA, CIA, and DoD (Department of Defense) databases." In Merkel's case, there are more than 300 reports from the year 2009 in which the chancellor is mentioned. The content of these reports is not included in the documents, but according to a Nymrod description from 2008, the database is a collection of "SIGINT-Targets." SIGINT stands for signals intelligence.

Collection Sites in Germany

Is it possible that the German government really knew nothing about all of these NSA activities within Germany? Are they really -- as they claimed in August 2013 in response to a query from the center-left Social Democratic Party (SPD) -- "unaware of the surveillance stations used by the NSA in Germany"?

That is difficult to believe, especially given that the NSA has been active in Germany for decades and has cooperated closely with the country's foreign intelligence agency, the BND, which is overseen by the Chancellery. A top-secret NSA paper from January 2013 notes: "NSA established a relationship with its SIGINT counterpart in Germany, the BND-TA, in 1962, which includes extensive analytical, operational, and technical exchanges."

When the cooperation with its junior partner from West Germany began, the NSA was just 10 years old and maintained stations in Augsburg and West Berlin in addition to its European headquarters in Stuttgart-Vaihingen.

American intelligence agencies, like those of the three other World War II victors, immediately began to monitor Germans within their zones of occupation, as confirmed by internal guidelines relating to the evaluation of reports stemming from the years 1946 to 1967.

In 1955, the British and French reduced their surveillance of Germans and focused on operations further to the east. The Americans, however, did not and continued to monitor telephone and other transmissions both within Germany and between the country and others in Western Europe. By the mid 1950s, US spies may have been listening in on some 5 million telephone conversations per year in Germany.

The easternmost NSA surveillance post in Europe during the Cold War was the Field Station Berlin, located on Teufelsberg (Devil's Mountain) in West Berlin. The hill is made from the rubble left over from World War II -- and the agents operating from its top were apparently extremely competent. They won the coveted Travis Trophy, awarded by the NSA each year to the best surveillance post worldwide, four times.

'A Perpetual State of Domination'

Josef Foschepoth, a German historian, refers to German-American relations as "a perpetual state of domination." He speaks of a "common law developed over the course of 60 years" allowing for uncontrolled US surveillance in Germany. Just how comprehensive this surveillance was -- and

remains -- can be seen from the so-called SIGAD lists, which are part of the Snowden archive. SIGAD stands for "Signal Intelligence Activity Designator" and refers to intelligence sources that intercept radio or telephone signals. Every US monitoring facility carries a code name made up of letters and numbers.

Documents indicate that the Americans often opened new SIGAD facilities and closed old ones over the decades, with a total of around 150 prior to the fall of the Wall. The technology used for such surveillance operations has advanced tremendously since then, with modern fiber-optic cables largely supplanting satellite communications. Data has become digital, making the capture of large quantities of it far easier.

The Snowden documents include a 2007 list that goes all the way back to 1917 and includes the names of many former and still active US military installations as well as other US facilities that are indicated as sites of data collection. It notes that a number of the codes listed are no longer in operation, and a deactivation date is included for at least a dozen. In other instances, the document states that the closing date is either unknown or that the SIGADs in question are still in operation. These latter codes include sites in Frankfurt, Berlin, Bad Aibling and Stuttgart -- all places still known to have an active NSA presence.

Because Americans tended to monitor their targets themselves, Germany's BND long had little to offer, creating a largely one-sided relationship in which the Germans played the subservient role. Only at the beginning of the last decade did the nature of the cooperation begin to change, partially as a result of the BND's successful effort to massively upgrade its technical abilities, as an internal NSA document notes approvingly. But the pecking order in the relationship has remained constant.

The former East Germany appears to have been better informed about the NSA's spying activities than Berlin currently claims to be. The NSA's work was known to the Hauptverwaltung Aufklärung (HVA), East Germany's foreign intelligence agency, a unit of the Ministry for State Security, the secret police more commonly known as the "Stasi." One internal Stasi document noted of the NSA: "This secret intelligence service of the USA saves all radio signals, conversations, etc., around the globe from friends and foes."

At the beginning of 1990, right after the Berlin Wall fell, HVA officers delivered around 40 binders with copies of NSA documents -- obtained by two spies -- to the Stasi's central archive. The HVA officers wanted to preserve the highly controversial material for historians and others who might be interested in it.

Not Enough for the USA

After US diplomats were informed by the German Federal Prosecutor of the documents' existence, Washington began applying pressure on the German government to hand over the NSA files. Finally, in July 1992, employees of the German agency responsible for executing the Stasi archive handed "two sealed containers with US documents" over to the German Federal Border Guard, which in turn delivered them to the Interior Ministry. Once in possession of them, the Americans used the files as evidence in the trial against a former NSA employee who had spied for East Germany.

Apparently the first haul of documents wasn't enough for the NSA. In 2008, during Merkel's first term in office, several NSA employees visited the Stasi archives to view all the remaining documents -- from the Stasi's Main Department III, which was responsible for signals intelligence -- containing information about US facilities.

The German Interior Ministry classified and blocked access to most of the material and they are no longer viewable by journalists or researchers. By the time Edward Snowden began publishing the NSA documents last year, only two files pertaining to the NSA remained available for viewing, and both were filled with harmless material. It is unlikely the remaining historical documents will be much help to the federal prosecutors now investigating the NSA.

But one person who could potentially contribute to clarifying the NSA's role in Germany was in Munich this week. General Keith Alexander, who recently left his position as NSA chief, spoke at a conference organized by Deutsche Telekom on Monday night. When officials at the Federal Prosecutor's Office were asked days before his keynote speech whether they would try to question

Alexander as a witness, they, responded by saying, "We do not conduct criminal investigative proceedings publicly."

It seems Germany's chief federal investigator may ultimately follow the dictum given by Foschepoth: "The German government is more concerned about keeping the Americans happy than it is about our constitution."

By Sven Becker, Hubert Gude, Judith Horchert, Andy Müller-Maguhn, Laura Poitras, Ole Reißmann, Marcel Rosenbach, Jörg Schindler, Fidelius Schmid, Michael Sontheimer and Holger Stark

Translated from the German by Charles Hawley and Daryl Lindsey

URL:

http://www.spiegel.de/international/germany/new-snowden-revelations-on-nsa-spying-in-germany-a-975441.html

Related SPIEGEL ONLINE links:

The NSA in Germany: Snowden's Documents Available for Download (06/18/2014)
http://www.spiegel.de/international/the-germany-file-of-edward-snowden-documents-available-for-download-a-975917.html

Abbreviations Explained: How to Read the NSA Documents (06/18/2014)
http://www.spiegel.de/international/world/glossary-of-nsa-abbreviations-a-975930.html

Spying Together: Germany's Deep Cooperation with the NSA (06/18/2014)
http://www.spiegel.de/international/germany/the-german-bnd-and-american-nsa-cooperate-more-closely-than-thought-a-975445.html

NSA in Germany: Why We Are Posting Secret Documents (06/18/2014)
http://www.spiegel.de/international/germany/why-spiegel-is-posting-leaked-nsa-documents-about-germany-a-975431.html

Interview with Ex-Stasi Agent: 'The Scope of NSA Surveillance Surprised Me' (06/18/2014)
http://www.spiegel.de/international/germany/interview-with-former-stasi-agent-about-the-nsa-a-975010.html

Snowden's Lawyer: 'Mutually Agreed Solution with US Would Be Most Sensible' (05/28/2014)
http://www.spiegel.de/international/germany/german-snowden-lawyer-says-whistleblower-negotiating-with-us-a-971790.html

Merkel's Mobile: Germany Launches Investigation into NSA Spying (06/04/2014)
http://www.spiegel.de/international/germany/germany-expected-to-open-investigation-into-nsa-spying-on-merkel-a-973326.html

'Risks': Snowden's Lawyer Expresses Concerns about Testimony (05/19/2014)
http://www.spiegel.de/international/germany/snowden-lawyer-expresses-doubts-about-testimony-in-nsa-probe-a-970213.html

Former NSA Director: 'Shame On Us' (03/24/2014)
http://www.spiegel.de/international/world/spiegel-interview-with-former-nsa-director-michael-hayden-a-960389.html

German Minister: 'US Operating Without any Kind of Boundaries' (04/09/2014)
http://www.spiegel.de/international/germany/german-interior-minister-warns-us-spying-has-no-boundaries-a-963179.html

Embassy Espionage: The NSA's Secret Spy Hub in Berlin (10/27/2013)
http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html

'Key Partners': Secret Links Between Germany and the NSA (07/22/2013)
http://www.spiegel.de/international/world/german-intelligence-worked-closely-with-nsa-on-data-surveillance-a-912355.html

Cover Story: How the NSA Targets Germany and Europe (07/01/2013)
http://www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609.html

SPIEGEL ONLINE
06/18/2014 04:21 PM

The NSA in Germany

Snowden's Documents Available for Download

In Edward Snowden's archive on NSA spying activities around the world, there are numerous documents pertaining to the agency's operations in Germany and its cooperation with German agencies. SPIEGEL is publishing 53 of them, available as PDF files.

America's National Security Agency has been active in Germany for decades. During the Cold War, much of its focus was on targets beyond West Germany's eastern border. But even then, the NSA continued to monitor communications within, and originating in, West Germany. Since the terror attacks of Sept. 11, 2001, the NSA has increased its ability to monitor global communications -- and documents from the archive of whistleblower Edward Snowden show that Germany is the agency's most important base of operations in continental Europe.

The documents show that the NSA, while focusing on counter-terrorism and other areas of importance to national security, has also established systems that allow it to monitor vast amounts of digital and other forms of communications in Germany and elsewhere. The agency can intercept huge amounts of emails, text messages and phone conversations. The NSA even monitored the mobile phone of German Chancellor Angela Merkel.

When revelations of NSA spying in Germany first broke last year, German officials indicated they were unaware of the breadth of US intelligence activity in the country. For this week's cover story, SPIEGEL once again examined all of the documents from Snowden's archive pertaining to NSA activity in Germany. The story can be read here.

But Snowden documents also indicate that Germany's foreign intelligence agency, the BND, and its domestic intelligence agency, the BfV, work closely together with the NSA in sites around Germany. For SPIEGEL's story on that cooperation, click here.

Below are PDF files of the most important documents pertaining to that cooperation. SPIEGEL has redacted them to obscure the identification of BND and NSA agents, phone numbers, email addresses and other information that could put lives in danger. A glossary explaining many of the abbreviations found in the documents can be found here. SPIEGEL's editorial explaining why we have elected to publicize the documents can be read here.

Please note, in some of the documents, you may have to scroll down to get to the text.

URL:

http://www.spiegel.de/international/the-germany-file-of-edward-snowden-documents-available-for-download-a-975917.html

Related SPIEGEL ONLINE links:

New NSA Revelations: Inside Snowden's Germany File (06/18/2014)
http://www.spiegel.de/international/germany/new-snowden-revelations-on-nsa-spying-in-germany-a-975441.html

Spying Together: Germany's Deep Cooperation with the NSA (06/18/2014)
http://www.spiegel.de/international/germany/the-german-bnd-and-american-nsa-cooperate-more-closely-than-thought-a-975445.html

NSA in Germany: Why We Are Posting Secret Documents (06/18/2014)
http://www.spiegel.de/international/germany/why-spiegel-is-posting-leaked-nsa-documents-about-germany-a-975431.html

Abbreviations Explained: How to Read the NSA Documents (06/18/2014)
http://www.spiegel.de/international/world/glossary-of-nsa-abbreviations-a-975930.html

(C//REL) TEMPORA -- "The World's Largest XKEYSCORE" -- Is Now Available to Qualified NSA Users

FROM: (U//FOUO) [redacted]
NSA Integree at GCHQ
Run Date: 09/19/2012

(U//FOUO) SIGINT analysts: We have all heard about Big Data; now you can get **Big Access** to Big Data.

(TS//SI//REL) What happens when one site contains more data than all other XKEYSCOREs combined? At more than 10 times larger than the next biggest XKEYSCORE,* **TEMPORA at GCHQ** is the world's largest XKEYSCORE and the NSA workforce is now getting greater access to it. This massive site uses over 1000 machines to process and make available to analysts more than 40 billion pieces of content a day. And starting today, skilled NSA XKEYSCORE users can get access to the TEMPORA database via the XKS-Central interface.

(TS//SI//REL) **What is TEMPORA?** TEMPORA is GCHQ's XKEYSCORE "Internet buffer" which exploits the most valuable Internet links available to GCHQ. TEMPORA provides a powerful discovery capability against Middle East, North African and European target sets (among others). Analysts who have benefited from GCHQ Special Source accesses like INCENSER or MUSCULAR will almost certainly benefit from TEMPORA.

(TS//SI//REL) **How valuable is TEMPORA?** The value and utility of TEMPORA were proven early into a 5-month evaluation that began this past March. With a limited user base of 300 analysts, TEMPORA became the second most valuable XKEYSCORE access for discovery. Additionally, this small group of analysts produced over 200 end-product reports and provided critical support to SIGINT, defensive, and cyber mission elements.

(TS//SI//REL) **Why TEMPORA?** TEMPORA provides the ability to do content-based discovery and development across a large array of high-priority signals. Similar to other XKEYSCORE deployments, TEMPORA effectively "slows down" a large chunk of Internet data, providing analysts with three working days to use the surgical toolkit of the GENESIS language to discover data that otherwise would have been missed. This tradecraft of ***content-based discovery*** using the GENESIS language is a critical tool in the analyst's discovery tool kit, and nicely complements the existing and well-known tradecrafts of strong selection targeting and bulk meta-data analysis.

(TS//SI//REL) **How do I get an account?** To comply with GCHQ policy and to ensure users are successful in such a large-scale environment, TEMPORA access requires users to be proficient with XKEYSCORE. At NSA this is achieved via the completion of various XKS Skilz achievements. Beginning today, users will see a new "TEMPORA" achievement, which requires users to have remained current with their UK Legalities training (OVSC1700), be a level 3 or higher XKS Skilz user, and have used GENESIS by either querying or authoring fingerprints. Users who meet those criteria will automatically be given TEMPORA access in their XKS Central account.

(S//SI//REL) **What do I need to know about using TEMPORA?** Although TEMPORA will appear as an additional database in XKS Central, there are some important items analysts need to be aware of when they search this database. Analysts are asked to pay close attention to details concerning the UK Legality requirements on the TEMPORA user-guidance wiki page. TEMPORA queries must comply with both UK and U.S. legal requirements, and the analytic community must ensure we are using this access wisely and compliantly.

(S//SI//REL) **How can I learn more about using XKEYSCORE?** If you'd like to get TEMPORA access but need some help fulfilling the proficiency requirements, the XKEYSCORE Outreach Team is ready to help. The team recently added an additional round of XKEYSCORE training sessions on ERS, which users can sign up for via this link. Also, analysts can find great tradecraft and training tips via the XKEYBLOG, or they can contact the team directly at DL XKS_Mentoring.

(U//FOUO) For more information **"go TEMPORA"** or contact [redacted]

(U) Notes:

* (S//SI/REL) XKEYSCORE is a computer-network exploitation system that combines high-speed filtering with SIGDEV. XKEYSCORE performs filtering and selection to enable analysts to quickly find information they need based on what they already know, but it also performs SIGDEV functions such as target development to allow analysts to discover new sources of information.

[edit] News

BREAKING NEWS (May 2012) - The second tranche of 'deep dive' processing capability at RPC has gone live. In addition 2 extra 10G's are being processed at OPC. This brings the current 'deep dive' capability to:

- CPC with 16 x 10g,
- OPC with 7 x 10g
- RPC1 with 23 x 10g.

This gives over 300 GCHQ and ~250 NSA analysts access to huge amounts of data to support the target discovery mission.

The MTI programme would like to say a big thanks to everyone who has made this possible (Which includes MTI [redacted] TGA, TEA, SSMG, SSOS, GTE, ACD, OPP-LEG, IT Services, R1 at NSA, AHS and [redacted]) - a true collaborative effort!

TEMPORA was delivered by the MTI Enhanced Discovery swimlane, led by [redacted] is part of the MTI SIGINT Apps theme led by [redacted] ([redacted] PM) and [redacted] ([redacted]

[edit] TEMPORA

TEMPORA is an Internet Buffer capability being delivered by MTI, IPP and GTE for joint mission benefit. It builds upon the key success of the TINT experiment and will provide a vital unique

capability to MISD/MCE communities.

- TEMPORA is the codeword for GCHQs internet buffer business capability as a whole – which is the ability to loosely promote a % of traffic across GCHQs SSE access into a repository which will keep the content (and its associated metadata) for periods of time (approximately 3 days for content and up to 30 days for metadata) to allow retrospective analysis and forwarding to follow on systems.
- TEMPORA as a capability is *agnostic* of the technologies used to promote that traffic and to store that traffic and so should not be used as a codeword for the individual components (e.g XKS, MVR etc).
- At the moment the components include, amongst others, GCHQ SSE Access, POKERFACE sanitisation, XKS (in various configurations) and it will include MVR in the very near future.
- TEMPORA also covers the management of the rules used to promote traffic into the internet buffer capability.
- TEMPORA is not processing centre specific. At the moment there are instances of TEMPORA at all xPC (Namely CPC, OPC and RPC1). These should be referred to, when required, as OPC/CPC/RPC1 TEMPORA

[edit] A bit more detail

TEMPORA are GCHQ's large-scale, Deep Dive deployments on Special Source access (SSE). Deep Dive XKeyscores work by promoting loose categories of traffic (e.g., all web, email, social, chat, EA, VPN, VoIP...) from the bearers feeding the system and block all the high-volume, low value traffic (e.g., P2P downloads). This usually equates to ~30% of the traffic on the bearer. We keep the full sessions for 3 working days and the metadata for 30 days for you to query, using all the functionality that Keyscore offers to slice and dice the data. The aim is to put the best 7.5% of our access into TEMPORA's, comprising a mix of Deep Dive Keyscores and promotion of data based on IP subnet or technology type from across the entire MVR. At the moment, users are able to access 46x10Gs of data via existing Internet Buffers.. This is a lot of data! Not only that, but the long-running TINT program and our initial 3-month operational trial of the CPC Internet Buffer (the first operational Internet Buffer to be deployed) show that every area of ops can get real benefit from this capability, especially for target discovery and target development. Internet Buffers are different from TINT in that the latter is purely an experimental, research environment whereas Internet Buffers can be used operationally for EPR, Effects, enabling CNE etc.

For a more detailed depiction of how TEMPORA and TINT differs please see here.

[edit] Contacts

Name	Role
[redacted]	GTE XKS Senior User
	MTI SIGINT apps theme lead
	Enhanced Discovery Project Manager
	Enhanced Discovery XKS SME

XKeyscoreTabs XKS Development

Jump to: navigation, search

News	Getting an Account	Using XKeyscore	Training	XKS Development	XKS Contacts	Requirements	News Archive

Quick Links

- XKEYSCORE Main Page
- XKS @ scale on SSE
- Getting Strong-Selected Content into XKS
- Getting an XKS Account
- Using XKEYSCORE
- XKEYSCORE Training
- **XKEYSCORE Development**
- XKEYSCORE Contacts
- XKS News Archive
- XKS Requirements
- XKS Searches user guide
- XKS Results user guide
- XKS Approval process
- NFV in XKS
- Promotion from XKS
- Automatic Promotion from XKS
- XKS for CNE
- NSA XKeyscore Using XKS for CNE
- XKS Tech Dictionaries

Useful Links

- Mastering The Internet
- Transforming Analysis
- TINT
- GTE
- SD Home

v · d · a

Contents

[edit] XKS Upgrades

XKS is upgraded fortnightly on Thursday mornings between 0900-1100. If you can't log on or use the tool during this period, its because of this.

[edit] Guidance on microplugins

As you know, you can create microplugins to do different things: some perform advanced detection techniques to find types of traffic which can't be detected by keywords or regular expressions alone. Others identify and extract data fields into XKS's metadata table.

In the latter case, the extracted content fragments are stored in the metadata table for 30 days. It will depend on the precision and nature of the search criteria you have used as to how strongly – or weakly – selected that content will be.

If you are going to use search criteria that will extract data about people and store that in the metadata table, please consult OPPLEG before doing so. They will wish to understand the nature and scope of any data being stored in case it includes at least the names of individuals and the majority of the data is not believed to relate to probable intelligence targets. This would make this data particularly sensitive.

In addition, a quarterly check is now being made on all new microplugins which add data to the

metadata table to ensure they meet UK legal and policy requirements.

Please also be aware that usually microplugins are automatically shared with at least NSA and may also get deployed to other 2P XKS. By mid-2011 a new version of XKS should have been deployed where individual microplugins will still be deployed to every XKS, but they can be tagged not to run on certain XKS. The only exception is where you deploy a microplugin only to GTE's XKS fleet: these will not be visible to 2P partners.

[edit] Types of XKEYSCORE

There are currently three different types of XKS:

- **Traditional**
- **Stage 2**
- **Deep Dive**

They differ principally on where in the processing chain they sit, whether the data they receive has already been sessionised or not and whether they ingest all of the data they receive or whether they apply rules to only ingest some data.

[edit] Traditional

When XKS was first developed it was used to receive data from low data rate signals being processed through WEALTHYCLUSTER (WC). WC sessionised all the data on the link and presented it all to XKS. All data was ingested into XKS.

GCHQ has traditional XKS at many of our sites, including all of our Comsat, Terrestrial and SMO sites. The EREPO XKS is also a traditional XKS, though in that case data has been softly selected at the implant and sessionisation takes place in TERRAIN, rather than WC.

[edit] Stage 2

For higher data rates, a "Stage 2" XKS was developed to ingest data from TURMOIL. TURMOIL passes 5% of the packets to XKS which XKS then sessionizes. TURMOIL decides which 5% of packets to pass based on the following criteria:

- strong selection
- subnet promotion
- technology promotion
- e-mail domains
- persona session promotion (where if a strong selector is seen, 10 minutes' or 10 MB of data is collected)
- persona session collection (where the data is collected and forwarded to NSA's PINWALE but is also passed to the XKS)

This data is then sent to the Stage 2 XKS. All other data is lost.

Only JPC (MUSCULAR) at GCHQ uses a Stage 2 XKS.

[edit] Deep Dive

Deep Dive XKS was developed to prove that sessionisation at 10G data rates was possible. First it sessionises all data on a link. Then it promotes data using the GENESIS selection language to identify data types where we assess there is potential intelligence value and ingests those. The promotion process can make one of three decisions:

- Block data that is legally not allowed to be in the system – ie UK-UK traffic
- Allow data that is known to be wanted through use of promotion rules
- And then to drop any data that doesn't meet either of these

One of the experiments in TINT is seeking to identify where the best balance lies between what is kept and what is not. A factor in deciding how much data to keep is the scale of storage capacity that can be provided.

GCHQ already operates a number of Deep Dive XKS:

exchange.

(TS//SI//NF) **Germany:** Provision of XKEYSCORE software to the BfV will expand their ability to support NSA as we jointly prosecute CT targets. Technical support for XKEYSCORE will be provided by the BND as it involves CES equities that a non-technical partner could inadvertently place at risk. Based on our CA relationship with the BND, they are well aware of, and able to, protect those equities.

PRIMARY FORNSAT COLLECTION OPERATIONS

(U//FOUO) Dragons, Shrimp, and XKEYSCORE: Tales from the Land of Brothers Grimm

FROM: [redacted]
European Cryptologic Center, SIGDEV (F22)
Run Date: 04/13/2012

(S//REL) The European Cryptologic Center (ECC) sits quietly nestled amongst vineyards and farmlands on

ECC

the outskirts of Darmstadt, Germany. To the passing motorist, the facility looks like many of the other random U.S. government facilities in the area, with one exception. One can almost hear a discernable buzz of activity from the analysts of the ECC executing queries, authoring fingerprints, and consuming metadata garnered from XKEYSCORE (XKS). In the past three months, the ECC has tripled, and even quadrupled in some cases, the number of queries performed, the number of items pushed to PINWALE, and the number of sessions viewed. And these numbers continue to grow.*

ECC

(S//REL) What has been the cause of this flurry of success? The ECC points to a recent ***XKS training blitz in support of the Analytic Modernization Outreach Campaign to encourage discovery.*** In early March, ECC SIGDEV analysts held an XKS Circuit Training event designed to expose analysts to five, 20-minute one-on-one sessions in a circuit-type environment. This "speed dating" for XKS consisted of five stations covering topics titled "Intro to the GUI and Basic Queries," "Metadata Setup and Manipulation," "Content and Manipulation of Results," "Introduction to Fingerprints," and "Introduction to Microplugins."

(S//REL) Over four days, 68 students were walked through these topics with five different instructors, able to ask specific questions and get more comfortable with the tool. "Everyone likes a new toy, and there was a lot of excitement about it. They will at least try it against their target and see what they will get out of it," said [redacted] one of the instructors and a SIGDEV Analyst embedded in Africa Division.

(S//SI//REL) With traditional targeting, analysts cast their nets wide into the murky waters of network traffic and haul in anything that gets caught in the net. We are like Forrest Gump on his shrimping boat off the coast of Alabama pulling in a boot, toilet seat, seaweed, and there they are... three shrimp! We burn up a lot of resources getting those shrimp, those reportable documents or metadata used to expand target knowledge, and we deal with tons of toilet seats, the spam and other junk. Then, we repeat the same process and hopefully catch enough "shrimp" to have ourselves a little cocktail. XKS has become so important because with it, analysts can downsize their gigantic shrimping nets to tiny, handheld goldfish-sized nets and merely dip them into the oceans of data, working smarter and scooping out exactly what they want.

(U//FOUO) And a short, two-hour class is an easy gamble of time for the hopes of being able to work smarter and more efficiently. ECC analysts have been trading in their old nets for new ones and are thrilled with their catches. Discovery can only occur if people are willing to try new things, and more of our analysts are getting comfortable with leaping into the relatively unknown world of XKS.

(U//FOUO) "The first time I saw XKS, I said, 'Whoa!!' It is intimidating because you open it up and you see all these queries and fields," said [redacted] "We took the students from that response to being able to approach it and navigate around in it. They see it differently now and know it's not a seven-headed dragon." This gentle introduction has definitely enabled analysts to ease into XKS and get more comfortable, and with that it has radically changed the overall mentality towards

the tool.

(S//REL) ***Across the ECC, analysts wholeheartedly agree that the Circuit Training setup and content was a catalyst to give XKS a try or take existing users to the next level.*** The one-on-one setup provided a heavy injection of tool knowledge into each student. "Before the training, I was just happy to use it and not go to jail," said [redacted] a Circuit Training student and Arabic/French Language Analyst for CT (Counterterrorism). "Now, I feel comfortable in my ability to use it and NOT go to jail. I used to always ask someone to look over my query before I submitted it. Now, my hand doesn't need to be held."

(S//REL) That Circuit Training must be one tough training to pull off, you say? Not so, says [redacted] who spoke about the "off-the-shelf" nature of the training. "The framework was already developed by GCHQ, so it was simple for us to read over their notes, make it applicable to NSA, and conduct the training. We didn't have to spend time writing modules."

(TS//SI//REL) From the leadership level's perspective, the time invested sending analysts to the class had a tremendous return. [redacted], Tech Lead for the 50-person strong Africa Division, said, "The brevity of the class made it easy to send our people. Now we know exactly why we want to use it, and we have discovered new traffic and documents. Our analysts have been building hashes for document tracking and rolling them into fingerprints. We have been getting documents in XKS that we were not getting in our PINWALE queries. Just today analysts found reportable material from the Tunisian Ministry of Interior that was not from any selectors we were targeting. Now we know what we can do with XKS and exactly why we want to use it – to make these discoveries."

(S//REL) These discoveries are igniting a trend of using XKS on a daily basis. "For daily pulls, analysts go through TransX, PINWALE, and now XKS to see what's new for the day," [redacted] said.

(U//FOUO) Combine these exciting finds with the introduction of XKS Skilz points, and you can see why McDonald's teamed up with Monopoly years ago: people buy more and even super size their orders just to get game pieces. With the brainchild of Skilz, where analysts can earn points and unlock achievements for performing tasks in XKS, people are willing to try new things within the tool. Analysts think to themselves, "Using the Pivot Data feature will earn 30 points... I'm going to try it and see what happens." Discovery! Points! We have been lured by our geeky desire to unlock achievements and earn points, and bragging rights are everything.

(U//FOUO) "Definitely a number of users have gotten into the Skilz points. We have several people at level six. They see what they need to do to earn more points and start trying out different things," said [redacted] In fact, ECC analysts now have the highest average of Skilz points compared to all of the S2 product lines and have written the most fingerprints per-capita! Some people say that the potent combination of Skilz points, the Circuit Training, and the team of easily-accessible, on-site instructors is the secret to ECC's successes with XKS.

(U//FOUO) Maybe XKS is a seven-headed dragon as [redacted] mentioned. Big and scary? Sure. Strong and powerful? Oh yeah. But, the ECC is taming it, and it is ours

to do with whatever we like, including catching shrimp.

(U//FOUO) POC: [redacted]) ECC SIGDEV.

---

* (S//REL) Here are charts to illustrate the point:

(TS//SI//NF) PRISM (US-984XN) Based Reporting: June 2011 – May 2012

Sorted By # of PRISM-Based Reports Per OPI

OPI - Top Producers Issuing	PRISM-Based Reports	% Increase in PRISM-Based Reports Compared to June 2010-May2011	% Of All OPI Reporting Which Is PRISM-Based	% Points Change from June 2010 - May 2011 period	All Reports By OPI	Single-Source to PRISM	% of PRISM-Based Reports Which are Single Source
SCS (F6*, US-96*, US-97*, US-3219)	3723	Up 67%	20	+7 (up 54%)	18640	3040	82
S2I - Counterterrorism	3493	Up 5%	42	-2 (down 5%)	8242	2074	60
S2E - Middle East & Africa	2574	Up 47%	16	+2 (up 14%)	16537	1959	76
S2G - Combating Prolif	2092	Up 49%	30	+3 (up 11%)	6872	1395	67
NSAT (USJ-783*)	1690	Up 20%	30	+3 (up 11%)	5713	1319	78
S2A - [redacted]	1389	Up 8%	11	-1 (down 8%)	12445	1196	86
NSAG (USJ-800*)	1255	Down 8%	11	0 (no change)	11741	883	70
ECC (ESOC) (USJ-753*, USM-44)	1147	Up 6%	52	+2 (up 4%)	2217	922	80
S2C - Intl Sec Issues	1147	Up 75%	13	+5 (up 63%)	8989	861	75
S2D - Countering Frgn Intel	862	Up 40%	12	-5 (down 29%)	7089	545	63
S2F - Intl Crime & Narc	666	Up 41%	16	+2 (up 14%)	4122	497	75
S2B - [redacted]	634	Down 10%	13	-3 (down 19%)	4842	452	71
NTOC (V*)	455	Up 237%	21	+8 (up 62%)	2195	355	78
DSD	310	Down 15%	4	0 (no change)	7511	296	95
NSAH (USJ-750*)	237	Down 10%	2	+1 (up 50%)	12023	155	65
S2J - Weapons and Space	225	Up 221%	33	+11 (50%)	692	186	83
GCHQ	197	Up 137%	2	+1.9 (up 1900%)	11257	170	86
S2H - [redacted]	176	Up 159%	5	+3 (up 150%)	3353	155	88
SSG	16	Up 60%	17	-19 (down 52%)	92	14	88
Utah Regional Ops Cntr (USJ-755)	12	Up 20%	6	-17 (down 74%)	207	12	100

Source: PLUS - 11-13 June 2012

(TS//SI//NF) PRISM (US-984XN) Based Reporting: June 2011 – May 2012

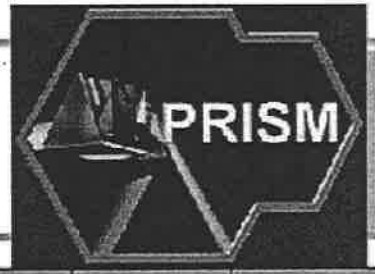
Sorted By % of PRISM-Based Reporting Per OPI

OPI - Top Producers Issuing	PRISM-Based Reports	% Increase in PRISM-Based Reports Compared to June 2010-May2011	% Of All OPI Reporting Which is PRISM-Based	% Points Change from June 2010 - May 2011 period	All Reports By OPI	Single-Source to PRISM	% of PRISM-Based Reports Which are Single Source
ECC (ESOC) (USJ-753*, USM-44)	1147	Up 6%	52	+2 (up 4%)	2217	922	80
S2I - Counterterrorism	3493	Up 5%	42	-2 (down 5%)	8242	2074	60
S2J - Weapons and Space	225	Up 221%	33	+11 (50%)	692	186	83
S2G - Combating Prolif	2092	Up 49%	30	+3 (up 11%)	6872	1395	67
NSAT (USJ-783*)	1690	Up 20%	30	+3 (up 11%)	5713	1319	78
NTOC (V*)	455	Up 237%	21	+8 (up 62%)	2195	355	78
SCS (F6*, US-96*, US-97*, US-3219)	3723	Up 67%	20	+ 7 (up 54%)	18640	3040	82
SSG	16	Up 60%	17	-19 (down 52%)	92	14	88
S2E - Middle East & Africa	2574	Up 47%	16	+2 (up 14%)	16537	1959	76
S2F - Intl Crime & Narc	666	Up 41%	16	+2 (up 14%)	4122	497	75
S2C - Intl Sec Issues	1147	Up 75%	13	+5 (up 63%)	8989	861	75
S2B - [redacted]	634	Down 10%	13	-3 (down 19%)	4842	452	71
S2D - Countering Fron Intel	862	Up 40%	12	-5 (down 29%)	7089	545	63
S2A - [redacted]	1389	Up 8%	11	-1 (down 8%)	12445	1196	86
NSAG (USJ-800*)	1255	Down 8%	11	0 (no change)	11741	883	70
Utah Regional Ops Cntr (USJ-755)	12	Up 20%	6	-17 (down 74%)	207	12	100
S2H - [redacted]	176	Up 159%	5	+3 (up 150%)	3353	155	88
DSD	310	Down 15%	4	0 (no change)	7511	296	95
NSAH (USJ-750*)	237	Down 10%	2	+1 (up 50%)	12023	155	65
GCHQ	197	Up 137%	2	+1.9 (up 1900%)	11257	170	86

Source: PLUS - 11-13 June 2012

FAA702 UTT DNI Tasking

Snapshot on 30 Jan 2013



Product Line	All DNI Selectors Tasked	DNI Selectors Tasked to SSO_CT_N (FAA/PRISM)	% of DNI Selectors Tasked to FAA/PRISM	% Points Change From Dec 2011	Increase in number of selectors tasked to FAA/PRISM Compared to Dec2011
S2A	9650	987	10%	-5	+232
S2B	12872	2263	18%	+6	+842
S2C	8763	1059	12%	+3	+468
S2D	10846	3796	35%	+11	+1872
S2E	18061	6935	38%	-4	+938
S2F	3577	1011	28%	+2	+423
S2G	12788	4172	33%	+2	+1019
S2H	10497	828	8%	+6	+660
S2I	14945	11461	77%	-1	+818
S2J	1077	242	22%	-2	-55
ECC (F22)	4880	3523	72%	-1	+715
FTS	7194	2402	33%	+9	+1126
FTV	68	0	0%	--	0
FGS	6919	3114	45%	-6	-17
FGV	127	50	39%	+21	+16

Product Line	All DNI Selectors Tasked	DNI Selectors Tasked to SSO_CT_N (FAA/PRISM)	% of DNI Selectors Tasked to FAA/PRISM	% Points Change From Dec 2011	Increase in number of selectors tasked to FAA/PRISM Compared to Dec2011
FHS	6101	612	10%	-7	+29
FCS	592	55	9%	+7	+52
F6	29476	4007	14%	--	+1650
F1Z – CSG CENTCOM	105	3	3%	-10	-46
F74 - MOC	300	171	57%	-7	-136
F7A - AMOC	417	6	1%	+1	+6
F7U - UROC	926	27	3%	--	-15
NTOC – V24	278	0	0%	--	0
NTOC – V25	30	17	57%	+39	+16
NTOC – V26/V23	4237	2814	66%	+4	+1490
NTOC – V32	2388	12	1%	+1	+11
NTOC – V35	15	0	0	--	0
SSG	6609	0	0%	--	0
S32	1388	86	6%	+1	+36

DNR realms excluded from UTT query: IMEI, IMSI, ituE.164, Ki.

Source: UTT Team

The Washington Post

National Security

NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say

By Barton Gellman and Ashkan Soltani October 30, 2013

The National Security Agency has secretly broken into the main communications links that connect Yahoo and Google data centers around the world, according to documents obtained from former NSA contractor Edward Snowden and interviews with knowledgeable officials.

By tapping those links, the agency has positioned itself to collect at will from hundreds of millions of user accounts, many of them belonging to Americans. The NSA does not keep everything it collects, but it keeps a lot.

According to a top-secret accounting dated Jan. 9, 2013, the NSA's acquisitions directorate sends millions of records every day from internal Yahoo and Google networks to data warehouses at the agency's headquarters at Fort Meade, Md. In the preceding 30 days, the report said, field collectors had processed and sent back 181,280,466 new records — including "metadata," which would indicate who sent or received e-mails and when, as well as content such as text, audio and video.

The NSA's principal tool to exploit the data links is a project called MUSCULAR, operated jointly with the agency's British counterpart, the Government Communications Headquarters . From undisclosed interception points, the NSA and the GCHQ are copying entire data flows across fiber-optic cables that carry information

among the data centers of the Silicon Valley giants.

The infiltration is especially striking because the NSA, under a separate program known as PRISM, has front-door access to Google and Yahoo user accounts through a court-approved process.

The MUSCULAR project appears to be an unusually aggressive use of NSA tradecraft against flagship American companies. The agency is built for high-tech spying, with a wide range of digital tools, but it has not been known to use them routinely against U.S. companies.

In a statement, the NSA said it is "focused on discovering and developing intelligence about valid foreign intelligence targets only."

"NSA applies Attorney General-approved processes to protect the privacy of U.S. persons — minimizing the likelihood of their information in our targeting, collection, processing, exploitation, retention, and dissemination," it said.

In a statement, Google's chief legal officer, David Drummond, said the company has "long been concerned about the possibility of this kind of snooping" and has not provided the government with access to its systems.

"We are outraged at the lengths to which the government seems to have gone to intercept data from our private fiber networks, and it underscores the need for urgent reform," he said.

A Yahoo spokeswoman said, "We have strict controls in place to protect the security of our data centers, and we have not given access to our data centers to the NSA or to any other government agency."

Under PRISM, the NSA gathers huge volumes of online communications records by legally compelling U.S. technology companies, including Yahoo and Google, to turn over any data that match court-approved search terms. That program, which was first

disclosed by The Washington Post and the Guardian newspaper in Britain, is authorized under Section 702 of the FISA Amendments Act and overseen by the Foreign Intelligence Surveillance Court (FISC).

Intercepting communications overseas has clear advantages for the NSA, with looser restrictions and less oversight. NSA documents about the effort refer directly to "full take," "bulk access" and "high volume" operations on Yahoo and Google networks. Such large-scale collection of Internet content would be illegal in the United States, but the operations take place overseas, where the NSA is allowed to presume that anyone using a foreign data link is a foreigner.

Outside U.S. territory, statutory restrictions on surveillance seldom apply and the FISC has no jurisdiction. Senate Intelligence Committee Chairman Dianne Feinstein (D-Calif.) has acknowledged that Congress conducts little oversight of intelligence-gathering under the presidential authority of Executive Order 12333 , which defines the basic powers and responsibilities of the intelligence agencies.

John Schindler, a former NSA chief analyst and frequent defender who teaches at the Naval War College, said it is obvious why the agency would prefer to avoid restrictions where it can.

"Look, NSA has platoons of lawyers, and their entire job is figuring out how to stay within the law and maximize collection by exploiting every loophole," he said. "It's fair to say the rules are less restrictive under Executive Order 12333 than they are under FISA," the Foreign Intelligence Surveillance Act.

In a statement, the Office of the Director of National Intelligence denied that it was using executive authority to "get around the limitations" imposed by FISA.

The operation to infiltrate data links exploits a fundamental weakness in systems architecture. To guard against data loss and system slowdowns, Google and Yahoo maintain fortresslike data centers across four continents and connect them with

thousands of miles of fiber-optic cable. Data move seamlessly around these globe-spanning "cloud" networks, which represent billions of dollars of investment.

For the data centers to operate effectively, they synchronize large volumes of information about account holders. Yahoo's internal network, for example, sometimes transmits entire e-mail archives — years of messages and attachments — from one data center to another.

Tapping the Google and Yahoo clouds allows the NSA to intercept communications in real time and to take "a retrospective look at target activity," according to one internal NSA document.

To obtain free access to data- center traffic, the NSA had to circumvent gold-standard security measures. Google "goes to great lengths to protect the data and intellectual property in these centers," according to one of the company's blog posts, with tightly audited access controls, heat-sensitive cameras, round-the-clock guards and biometric verification of identities.

Google and Yahoo also pay for premium data links, designed to be faster, more reliable and more secure. In recent years, both of them are said to have bought or leased thousands of miles of fiber-optic cables for their own exclusive use. They had reason to think, insiders said, that their private, internal networks were safe from prying eyes.

In an NSA presentation slide on "Google Cloud Exploitation," however, a sketch shows where the "Public Internet" meets the internal "Google Cloud" where their data reside. In hand-printed letters, the drawing notes that encryption is "added and removed here!" The artist adds a smiley face, a cheeky celebration of victory over Google security.

Two engineers with close ties to Google exploded in profanity when they saw the

drawing. "I hope you publish this," one of them said.

For the MUSCULAR project, the GCHQ directs all intake into a "buffer" that can hold three to five days of traffic before recycling storage space. From the buffer, custom-built NSA tools unpack and decode the special data formats that the two companies use inside their clouds. Then the data are sent through a series of filters to "select" information the NSA wants and "defeat" what it does not.

PowerPoint slides about the Google cloud, for example, show that the NSA tries to filter out all data from the company's "Web crawler," which indexes Internet pages.

According to the briefing documents, prepared by participants in the MUSCULAR project, collection from inside Yahoo and Google has produced important intelligence leads against hostile foreign governments that are specified in the documents.

Last month, long before The Post approached Google to discuss the penetration of its cloud, Eric Grosse, vice president for security engineering, said the company is rushing to encrypt the links between its data centers. "It's an arms race," he said then. "We see these government agencies as among the most skilled players in this game."

Yahoo has not announced plans to encrypt its data-center links.

Because digital communications and cloud storage do not usually adhere to national boundaries, MUSCULAR and a previously disclosed NSA operation to collect Internet address books have amassed content and metadata on a previously unknown scale from U.S. citizens and residents. Those operations have gone undebated in public or in Congress because their existence was classified.

The Google and Yahoo operations call attention to an asymmetry in U.S. surveillance law. Although Congress has lifted some restrictions on NSA domestic surveillance on grounds that purely foreign communications sometimes pass over U.S. switches and cables, it has not added restrictions overseas, where American communications or data stores now cross over foreign switches.

"Thirty-five years ago, different countries had their own telecommunications infrastructure, so the division between foreign and domestic collection was clear," Sen. Ron Wyden (D-Ore.), a member of the intelligence panel, said in an interview. "Today there's a global communications infrastructure, so there's a greater risk of collecting on Americans when the NSA collects overseas."

It is not clear how much data from Americans is collected and how much of that is retained. One weekly report on MUSCULAR says the British operators of the site allow the NSA to contribute 100,000 "selectors," or search terms. That is more than twice the number in use in the PRISM program, but even 100,000 cannot easily account for the millions of records that are said to be sent to Fort Meade each day.

In 2011, when the FISC learned that the NSA was using similar methods to collect and analyze data streams — on a much smaller scale — from cables on U.S. territory, Judge John D. Bates ruled that the program was illegal under FISA and inconsistent with the requirements of the Fourth Amendment.

Soltani is an independent security researcher and consultant.

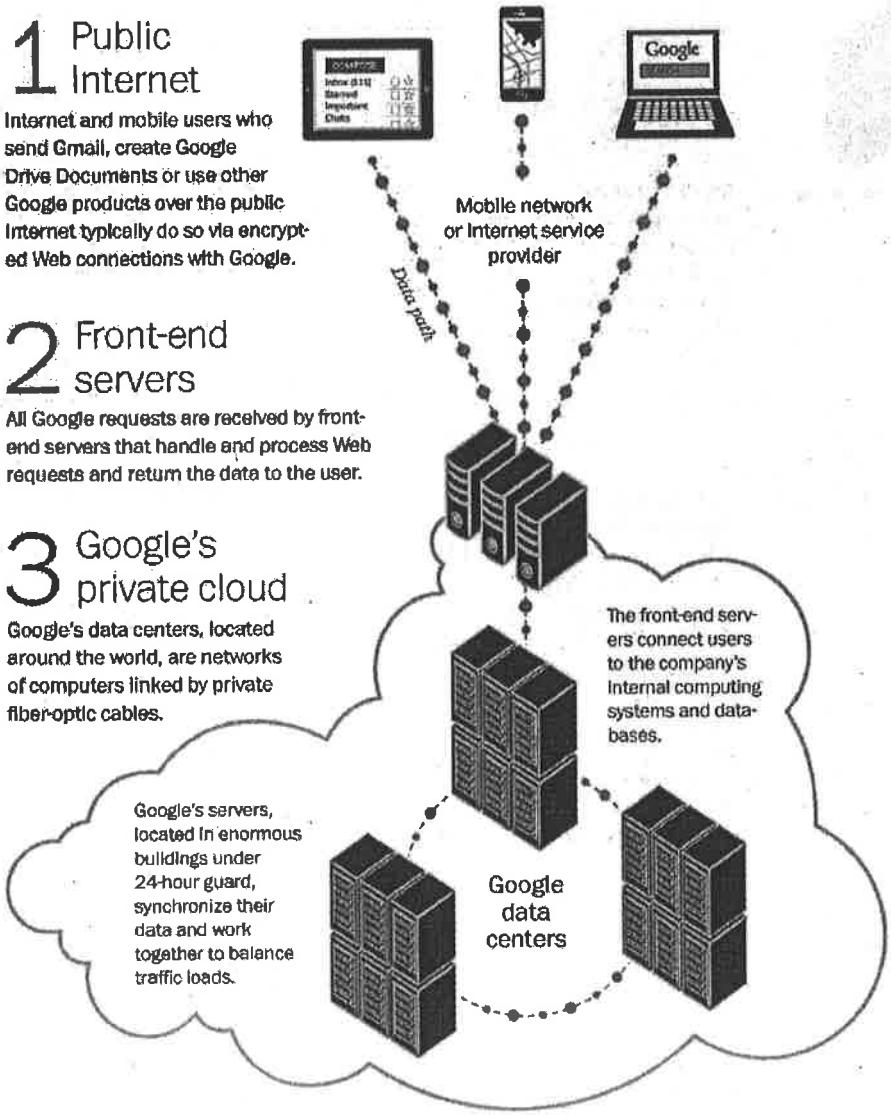
Barton Gellman writes for the national staff. He has contributed to three Pulitzer Prizes for The Washington Post, most recently the 2014 Pulitzer Prize for Public Service.

National Security

How the NSA is infiltrating private networks

By Barton Gellman, Todd Lindeman and Ashkan Soltani, Published: Oct. 30, 2013

The NSA, working with its British counterpart, the Government Communications Headquarters (GCHQ), secretly taps into the internal networks of Yahoo and Google, the two biggest Internet companies by overall data traffic. The operation intercepts information flowing between the enormous data centers that those companies maintain around the world. In general, Google and Yahoo use privately owned or leased lines to synchronize their data centers. This graphic shows how the NSA and GCHQ break into those internal networks, using Google's as an example. Less is known about Yahoo's networks, but the NSA operations are thought to be similar.



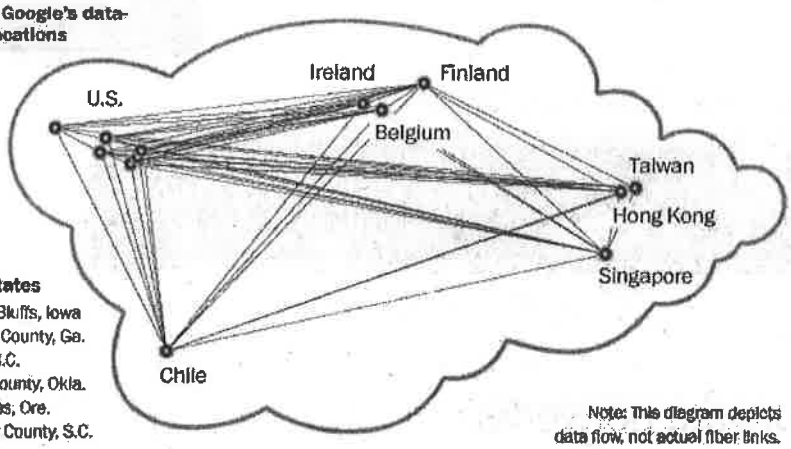
4 Google's global infrastructure

Cloud companies, such as Google and Yahoo, store multiple copies of user data across geographically distributed data centers in order to improve reliability and performance.

Google and Yahoo generally connect their data centers over privately owned or leased fiber-optic

cables, which do not share traffic with other Internet users and companies, to enable the fastest connections and keep information secure. Until recently, these internal data networks were not encrypted. Google announced in September, however, that it is moving quickly to encrypt those connections. Yahoo's data center links are not encrypted.

Some of Google's data-center locations

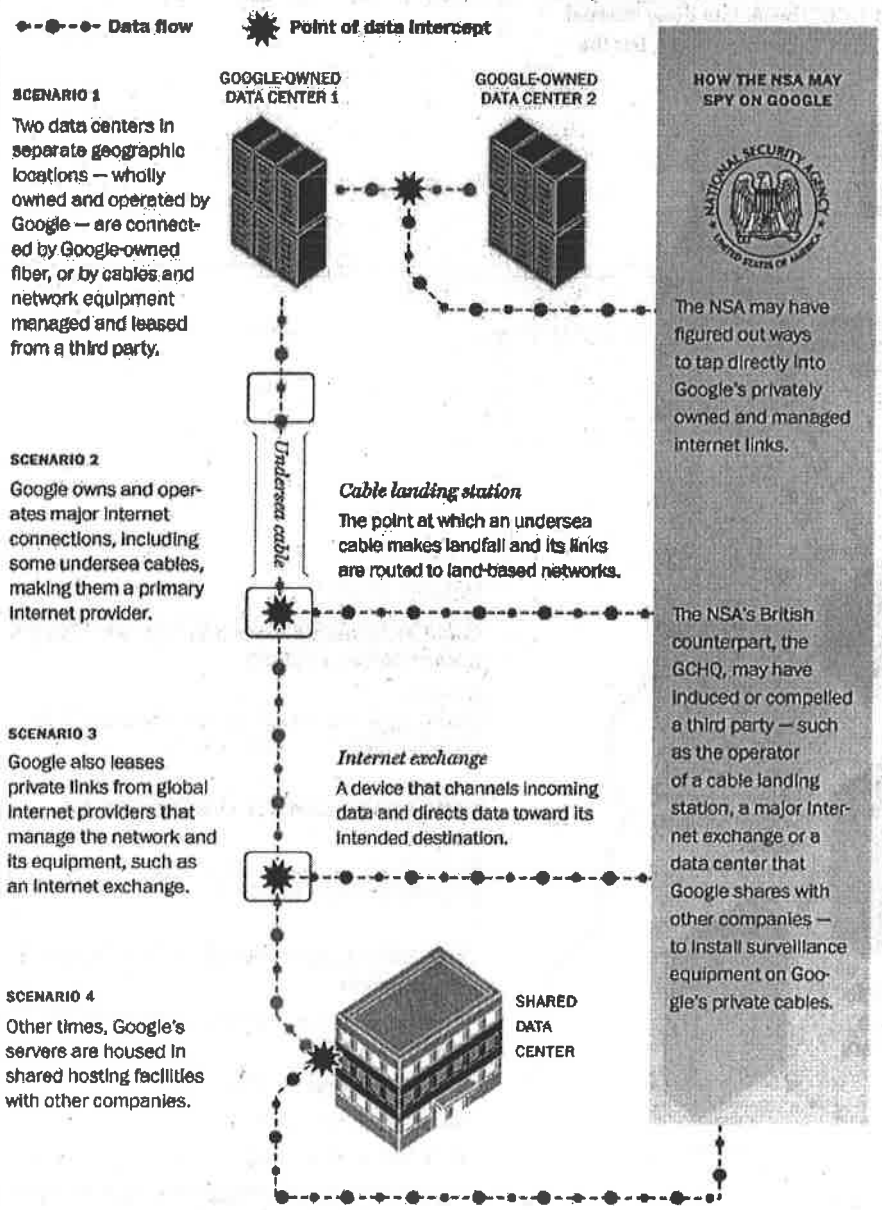


United States
- Council Bluffs, Iowa
- Douglas County, Ga.
- Lenoir, N.C.
- Mayes County, Okla.
- The Dalles, Ore.
- Berkeley County, S.C.

Note: This diagram depicts data flow, not actual fiber links.

5 How the NSA's spying on Google's internal network is intercepting data on Americans

The NSA intercepts user account information as it flows between data centers. The precise collection points and methods are unknown. These are among the possibilities:



SOURCE: Staff reports; Google, www.google.com/about/datacenters.

80 Comments Discussion Policy

Please Sign In to Comment ()

JUNE 2, 2014 | BY MARK JAYCOX

A Primer on Executive Order 12333: The Mass Surveillance Starlet

Many news reports have focused on Section 215 of the Patriot Act (used to collect all Americans' calling records) and Section 702 of the Foreign Intelligence Surveillance Act Amendments Act (FAA) (used to collect phone calls, emails and other Internet content) as the legal authorities supporting much of the NSA's spying regime. Both laws were passed by Congress and are overseen by the Foreign Intelligence Surveillance Court (FISA court). However, it's likely that the NSA conducts much more of its spying under the President's claimed inherent powers and only governed by a document originally approved by President Reagan titled Executive Order 12333. The Senate Select Committee on Intelligence is currently conducting a secret investigation into the order, but Congress as a whole—including the Judiciary committee—must release more information about the order to the public.

EO 12333 was first written in 1981 in the wake of Watergate and the Foreign Intelligence Surveillance Act, an act passed by Congress that regulates spying conducted on people located within the United States. Since FISA only covers specific types of spying, the President maintains that the executive branch remains free to spy abroad on foreigners with little to no regulation by Congress.

Executive Order 12333

The Executive Order does three things: it outlines what it governs, when the agencies can spy, and how they can spy. In broad strokes, the Executive Order mandates rules for spying on United States persons (a term that includes citizens and lawful permanent residents wherever they may be) and on anyone within the United States. It also directs the Attorney General and others to create further policies and procedures for what information can be collected, retained, and shared.

The first section of the order covers the role of every agency conducting intelligence in the Intelligence Community, which includes seventeen different agencies, including well-known entities like the Central Intelligence Agency (CIA) and the NSA, and lesser-known entities like the Office of Terrorism and Financial Intelligence in the Department of Treasury. The roles vary by agency. For instance, the NSA is, among other things, responsible for "collection, processing and dissemination of signals intelligence," while the CIA is responsible for "national foreign intelligence.

The Information Collected

The Executive Order purports to cover all types of spying conducted with the President's constitutional powers—including mass spying. That's important to note because some of the spying conducted under EO 12333 is reportedly similar to the mass spying conducted under Section 702 of the FAA. Under this type of spying, millions of innocent foreigners' communications are collected abroad, inevitably containing Americans' communications. In the Section 702 context, this includes techniques like Prism and Upstream. While we don't know for sure, the Executive Order probably uses similar techniques or piggybacks off of programs used for Section 702 spying.

The second section of the EO partly covers mass spying by establishing what information intelligence agencies can collect, retain, and share about US persons. The current guidelines, the United States Signals Intelligence Directive SP0018, also known as "USSID 18," are (just like

the "minimization procedures" based off of them) littered with loopholes to over-collect, over-retain, and over-share Americans' communications—all without a probable cause warrant or any judicial oversight.

Defenders (.pdf) of the mass spying conducted under the Executive Order point out the order "protects" such US person information with guidelines like USSID 18, but such protections are window-dressing, at best. Policies like USSID 18 and other accompanying Executive Order guidelines such as the "Special Procedures Governing Communications Metadata Analysis" allow for extensive use of US person information and data without a probable cause warrant. Indeed, news reports and Congressional testimony confirm the "Special Procedures" are used to map Americans' social networks. The procedures are clear evidence the government believes that Fourth Amendment's protections stop at the border.

Uses of Executive Order 12333

We do know a little about the spying conducted using EO 12333, but more must be revealed to the public. One early news report revealed it was the NSA's claimed authority for the collection of Americans' address books and buddy lists. It's also involved in the NSA's elite hacking unit, the Tailored Access Operations unit, which targets system administrators and installs malware while masquerading as Facebook servers. And in March, the Washington Post revealed the order alone—without any court oversight—is used to justify the recording of "100 percent of a foreign country's telephone calls." The NSA's reliance on the order for foreign spying includes few, if any, Congressional limits or oversight. Some of the only known limits on Executive spying are found in Executive procedures like USSID 18, the metadata procedures discussed above, and probably other still-classified National Security Policy Directives, none of which have been publicly debated much less approved by Congress or the courts.

The extent of the NSA's reliance on Executive Order 12333 demands that the government release more information about how the order is used, or misused. And Congress—specifically the Judiciary and Intelligence committees—must reassert the same aggressive and diligent oversight they performed in the 1970s and 1980s.

NSA Spying | Transparency

Global Chokepoints

HTTPS Everywhere

Medical Privacy Project

Open Wireless Movement

Patent Busting

Student Activism

Surveillance Self-Defense

Takedown Hall of Shame

Teaching Copyright

Transparency Project

Trolling Effects

Ways To Help

MORE DEEPLINKS POSTS LIKE THIS

MAY 2014
The Way the NSA Uses Section 702 is Deeply Troubling. Here's Why.

DECEMBER 2014
EFF Statement on the 2015 Intelligence Authorization Bill

APRIL 2014
An NSA "Reform Bill" of the Intelligence Community, Written by the Intelligence Community, and for the Intelligence Community

NOVEMBER 2013
Three Leaks, Three Weeks, and What We've Learned About the US Government's Other Spying Authority: Executive Order 12333

JULY 2012
Why The NSA Can't Be Trusted to Run U.S. Cybersecurity Programs

RECENT DEEPLINKS POSTS

FEB 27, 2015
Stupid Patent of the Month: Attorney "Inventor" Games the System

FEB 27, 2015
EFF Tells the Supreme Court that Patent Law Shouldn't Reward Ambiguity

FEB 26, 2015
Congress Is Poised to Introduce a Bill to Fast Track TPP so It's Time to Act Now

FEB 26, 2015
EFF to Congress: Curb Patent Demand Letter Abuse

FEB 26, 2015
Dear FCC: Thanks for Listening to Team Internet!

DEEPLINKS TOPICS

Fair Use and Intellectual Property: Defending the Balance
Free Speech
Innovation
DMCA Rulemaking
Do Not Track
DRM
E-Voting Rights
EFF Europe
Patent Trolls
Patents
PATRIOT Act
Pen Trap
Policy Analysis

Office of the Director of National Intelligence

Statistical Transparency Report Regarding use of National Security Authorities

Annual Statistics for Calendar Year 2013

~~Classified By: 2381928~~
~~Derived From: ODNI COL T-12~~
~~Reason:~~
~~Declassify On: 20391231~~

Statistical Transparency Report Regarding use of National Security Authorities

June 26, 2014

Introduction.

In June 2013, President Obama directed the Intelligence Community to declassify and make public as much information as possible about certain sensitive U.S. Government surveillance programs while protecting sensitive classified intelligence and national security information. Over the past year, the Director of National Intelligence (DNI) has declassified and authorized the public release of thousands of pages of documents relating to the use of critical national security authorities. Today, and consistent with the DNI's directive on August 29, 2013, we are releasing information related to the use of these important tools, and will do so in the future on an annual basis. Accordingly, the DNI has declassified and directed the release of the following information for calendar year 2013.

Annual Statistics for Calendar Year 2013 Regarding Use of Certain National Security Legal Authorities.

Titles I, III, IV, and VII of FISA.

Legal Authority	Annual Number of Orders	Estimated Number of Targets Affected
FISA Orders based on probable cause (Title I and III of FISA, Sections 703 and 704 of FISA)	1,767 orders	1,144
Section 702 of FISA	1 order	89,138
FISA Pen Register/Trap and Trace (Title IV of FISA)	131 orders	319

It is important to provide some additional context to the above statistics.

- **Targets.** Within the Intelligence Community, the term "target" has multiple meanings. For example, "target" could be an individual person, a group, or an organization composed of multiple individuals or a foreign power that possesses or is likely to communicate foreign intelligence information that the U.S. government is authorized to acquire by the above-referenced laws. Some laws require that the government obtain a Court order specifying the communications facilities used by a "target" to be subject to intelligence collection. Although the government may have legal authority to conduct intelligence collection against multiple communications facilities used by the target, the user of the facilities - the "target" - is only counted once in the above figures.

- **702 Targets.** In addition to the explanation of target above, in the context of Section 702 the term "target" is generally used to refer to the act of intentionally directing intelligence collection at a particular person, a group, or organization. For example, the statutory provisions of Section 702 state that the Government "may not *intentionally target any person* known at the time of the acquisition to be located in the United States" (emphasis added), among other express limitations. Under Section 702, the Foreign Intelligence Surveillance Court (FISC) approves Certifications as opposed to individualized orders. Thus, the number of 702 "targets" reflects an estimate of the number of known users of particular facilities (sometimes referred to as selectors) subject to intelligence collection under those Certifications. This estimate is based on the information readily available to the Intelligence Community to identify unique targets – users, whose identity may be unknown, but who are reasonably believed to use the particular facility from outside the United States and who are reasonably believed to be non-United States persons. For example, foreign intelligence targets often communicate using several different email accounts. Unless the Intelligence Community has information that multiple email accounts are used by the same target, each of those accounts would be counted separately in these figures. On the other hand, if the Intelligence Community is aware that the accounts are all used by the same target, as defined above, they would be counted as one target.

- **Relationship of Orders to Targets.** In some cases, one order can by its terms affect multiple targets (as with Section 702). Alternatively, a target may be the subject of multiple orders, as noted below.

- **Amendments and Renewals.** The FISC may amend an order one or more times after it has been issued. For example, an order may be amended to add a newly discovered account used by the target. To avoid redundant counting, these statistics do not count such amendments separately. Moreover, some orders may be renewed multiple times during the calendar year (for example, the FISA statute provides that a Section 704 FISA Order against a U.S. person target may last no longer than 90 days but permits the order to be renewed). The statistics count each such renewal as a separate order.

Title V of FISA (Business Records).

We are reporting information about the Government's use of the FISA Business Records provision (Title V) separately because this authority has been used in two distinct ways – collection of business records to obtain information about a specific subject and collection of business records in bulk. Accordingly, in the interest of transparency, we have decided to clarify the extent to which individuals are affected by each use. In addition, instead of reporting on the number of Business Record orders, the government is reporting on the number of *applications* submitted to the Foreign Intelligence Surveillance Court because the FISC may issue several orders to different recipients based upon a particular application.

Legal Authority	Annual Number of Applications	Estimated Number Affected
FISA Business Records (Title V of FISA)	178	172: The number of individuals, entities, or foreign powers subject to a business records application to obtain information about a specific subject
		423: The number of selectors approved to be queried under the NSA telephony metadata program
		248: The number of known or presumed U.S. persons who were the subject of queries of information collected in bulk or who were subject to a business records application.

National Security Letters.

Finally, we are reporting information on the Government's use of National Security Letters (NSLs). On April 30, 2014, the Department of Justice released its Annual Foreign Intelligence Surveillance Act Report to Congress. That report, which is available here reports on the number of requests made for certain information concerning different United States persons pursuant to NSL authorities during calendar year 2013. In addition to those figures, today we are reporting (1) the total number of NSLs issued for all persons, and (2) the total number of requests for information contained within those NSLs. For example, one NSL seeking subscriber information from one provider may identify three e-mail addresses, all of which are relevant to the same pending investigation and each is considered a "request."

We are reporting the annual number of requests rather than "targets" for multiple reasons. First, the FBI's systems are configured to comply with Congressional reporting requirements, which do not require the FBI to track the number of individuals or organizations that are the subject of an NSL. Even if the FBI systems were configured differently, it would still be difficult to identify the number of specific individuals or organizations that are the subjects of NSLs. One reason for this is that the subscriber information returned to the FBI in response to an NSL may identify, for example, one subscriber for three accounts or it may identify different subscribers for each account. In some cases this occurs because the identification information provided by the subscriber to the provider may not be true. For example, a subscriber may use a fictitious name or alias when creating the account. Thus, in many instances, the FBI never identifies the actual subscriber of a facility. In other cases this occurs because individual

subscribers may identify themselves differently for each account, e.g., inclusion of middle name, middle initial, etc., when creating an account.

We also note that the actual number of individuals or organizations that are the subject of an NSL is different than the number of NSL requests. The FBI often issues NSLs under different legal authorities, e.g., 12 U.S.C. § 3414(a)(5), 15 U.S.C. §§ 1681u(a) and (b), 15 U.S.C. § 1681v, and 18 U.S.C. § 2709, for the same individual or organization. The FBI may also serve multiple NSLs for an individual for multiple facilities, e.g., multiple e-mail accounts, landline telephone numbers, cellular phone numbers, etc. The number of requests, consequently, is significantly larger than the number of individuals or organizations that are the subjects of the NSLs.

Legal Authority	Annual Number of NSLs Issued	Annual Number of Requests for Information
National Security Letters issued pursuant to 12 U.S.C. § 3414(a)(5), 15 U.S.C. §§ 1681u(a) and (b), 15 U.S.C. § 1681v, and 18 U.S.C. § 2709	19,212	38,832

This information will be available at the website of the Office of the Director of National Intelligence (ODNI); and ODNI's public website dedicated to fostering greater public visibility into the intelligence activities of the Government, ICOntheRecord.tumblr.com.

The White House

Office of the Press Secretary

For Immediate Release January 17, 2014

Remarks by the President on Review of Signals Intelligence

Department of Justice
Washington, D.C.

11:15 A.M. EST

THE PRESIDENT: At the dawn of our Republic, a small, secret surveillance committee borne out of the "The Sons of Liberty" was established in Boston. And the group's members included Paul Revere. At night, they would patrol the streets, reporting back any signs that the British were preparing raids against America's early Patriots.

Throughout American history, intelligence has helped secure our country and our freedoms. In the Civil War, Union balloon reconnaissance tracked the size of Confederate armies by counting the number of campfires. In World War II, code-breakers gave us insights into Japanese war plans, and when Patton marched across Europe, intercepted communications helped save the lives of his troops. After the war, the rise of the Iron Curtain and nuclear weapons only increased the need for sustained intelligence gathering. And so, in the early days of the Cold War, President Truman created the National Security Agency, or NSA, to give us insights into the Soviet bloc, and provide our leaders with information they needed to confront aggression and avert catastrophe.

Throughout this evolution, we benefited from both our Constitution and our traditions of limited government. U.S. intelligence agencies were anchored in a system of checks and balances -- with oversight from elected leaders, and protections for ordinary citizens. Meanwhile, totalitarian states like East Germany offered a cautionary tale of what could happen when vast, unchecked surveillance turned citizens into informers, and persecuted people for what they said in the privacy of their own homes.

In fact, even the United States proved not to be immune to the abuse of surveillance. And in the 1960s, government spied on civil rights leaders and critics of the Vietnam War. And partly in response to these revelations, additional laws were established in the 1970s to ensure that our intelligence capabilities could not be misused against our citizens. In the long, twilight struggle against Communism, we had been reminded that the very liberties that we sought to preserve could not be sacrificed at the altar of national security.

If the fall of the Soviet Union left America without a competing superpower, emerging threats from terrorist groups, and the proliferation of weapons of mass destruction placed new and in some ways more complicated demands on our intelligence agencies. Globalization and the Internet made these threats more acute, as technology erased borders and empowered individuals to project great violence, as well as great good. Moreover, these new threats raised new legal and new policy questions. For while few doubted the legitimacy of spying on hostile states, our framework of laws was not fully adapted to prevent terrorist attacks by individuals acting on their own, or acting in small, ideologically driven groups on behalf of a foreign power.

The horror of September 11th brought all these issues to the fore. Across the political spectrum, Americans recognized that we had to adapt to a world in which a bomb could be built in a basement, and our electric grid could be shut down by operators an ocean away. We were shaken by the signs we had missed leading up to the attacks -- how the hijackers had made phone calls to known extremists and traveled to suspicious places. So we demanded that our intelligence community improve its capabilities, and that law enforcement change practices to focus more on preventing attacks before they happen than prosecuting terrorists after an attack.

It is hard to overstate the transformation America's intelligence community had to go through after 9/11. Our agencies suddenly needed to do far more than the traditional mission of monitoring hostile powers and gathering information for policymakers. Instead, they were now asked to identify and target plotters in some of the most remote parts of the world, and to anticipate the actions of networks that, by their very nature, cannot be easily penetrated with spies or informants.

And it is a testimony to the hard work and dedication of the men and women of our intelligence community that over the past decade we've made enormous strides in fulfilling this mission. Today, new capabilities allow intelligence agencies to track who a terrorist is in contact with, and follow the trail of his travel or his funding. New laws allow information to be collected and shared more quickly and effectively between federal agencies, and state and local law enforcement. Relationships with foreign intelligence services have expanded, and our capacity to repel cyber-attacks have been strengthened. And taken together, these efforts have prevented multiple attacks and saved innocent lives -- not just here in the United States, but around the globe.

And yet, in our rush to respond to a very real and novel set of threats, the risk of government overreach -- the

WATCH THE VIDEO

January 17, 2014 3:28 PM
President Obama Speaks on U.S. Intelligence Programs

LATEST BLOG POSTS

March 02, 2015 10:27 AM EST
The Faces of Health Care: Jason T.

March 02, 2015 9:30 AM EST
Previewing Vice President Biden's Trip to Guatemala
Continuing the Administration's active engagement in Central America, the Vice President is traveling to Guatemala City to meet with the Presidents of El Salvador, Guatemala, Honduras, and the President of the Inter-American Development Bank.

March 01, 2015 4:12 PM EST
5 Things You Need to Know About the U.S.-Israel Relationship Under President Obama
Under President Obama's leadership, American engagement with Israel has grown and strengthened to an unprecedented degree.

VIEW ALL RELATED BLOG POSTS

Facebook YouTube
Twitter Vimeo
Flickr iTunes
Google+ LinkedIn

possibility that we lose some of our core liberties in pursuit of security -- also became more pronounced. We saw, in the immediate aftermath of 9/11, our government engaged in enhanced interrogation techniques that contradicted our values. As a Senator, I was critical of several practices, such as warrantless wiretaps. And all too often new authorities were instituted without adequate public debate.

Through a combination of action by the courts, increased congressional oversight, and adjustments by the previous administration, some of the worst excesses that emerged after 9/11 were curbed by the time I took office. But a variety of factors have continued to complicate America's efforts to both defend our nation and uphold our civil liberties.

First, the same technological advances that allow U.S. intelligence agencies to pinpoint an al Qaeda cell in Yemen or an email between two terrorists in the Sahel also mean that many routine communications around the world are within our reach. And at a time when more and more of our lives are digital, that prospect is disquieting for all of us.

Second, the combination of increased digital information and powerful supercomputers offers intelligence agencies the possibility of sifting through massive amounts of bulk data to identify patterns or pursue leads that may thwart impending threats. It's a powerful tool. But the government collection and storage of such bulk data also creates a potential for abuse.

Third, the legal safeguards that restrict surveillance against U.S. persons without a warrant do not apply to foreign persons overseas. This is not unique to America; few, if any, spy agencies around the world constrain their activities beyond their own borders. And the whole point of intelligence is to obtain information that is not publicly available. But America's capabilities are unique, and the power of new technologies means that there are fewer and fewer technical constraints on what we can do. That places a special obligation on us to ask tough questions about what we should do.

And finally, intelligence agencies cannot function without secrecy, which makes their work less subject to public debate. Yet there is an inevitable bias not only within the intelligence community, but among all of us who are responsible for national security, to collect more information about the world, not less. So in the absence of institutional requirements for regular debate -- and oversight that is public, as well as private or classified -- the danger of government overreach becomes more acute. And this is particularly true when surveillance technology and our reliance on digital information is evolving much faster than our laws.

For all these reasons, I maintained a healthy skepticism toward our surveillance programs after I became President. I ordered that our programs be reviewed by my national security team and our lawyers, and in some cases I ordered changes in how we did business. We increased oversight and auditing, including new structures aimed at compliance. Improved rules were proposed by the government and approved by the Foreign Intelligence Surveillance Court. And we sought to keep Congress continually updated on these activities.

What I did not do is stop these programs wholesale -- not only because I felt that they made us more secure, but also because nothing in that initial review, and nothing that I have learned since, indicated that our intelligence community has sought to violate the law or is cavalier about the civil liberties of their fellow citizens.

To the contrary, in an extraordinarily difficult job -- one in which actions are second-guessed, success is unreported, and failure can be catastrophic -- the men and women of the intelligence community, including the NSA, consistently follow protocols designed to protect the privacy of ordinary people. They're not abusing authorities in order to listen to your private phone calls or read your emails. When mistakes are made -- which is inevitable in any large and complicated human enterprise -- they correct those mistakes. Laboring in obscurity, often unable to discuss their work even with family and friends, the men and women at the NSA know that if another 9/11 or massive cyber-attack occurs, they will be asked, by Congress and the media, why they failed to connect the dots. What sustains those who work at NSA and our other intelligence agencies through all these pressures is the knowledge that their professionalism and dedication play a central role in the defense of our nation.

Now, to say that our intelligence community follows the law, and is staffed by patriots, is not to suggest that I or others in my administration felt complacent about the potential impact of these programs. Those of us who hold office in America have a responsibility to our Constitution, and while I was confident in the integrity of those who lead our intelligence community, it was clear to me in observing our intelligence operations on a regular basis that changes in our technological capabilities were raising new questions about the privacy safeguards currently in place.

Moreover, after an extended review of our use of drones in the fight against terrorist networks, I believed a fresh examination of our surveillance programs was a necessary next step in our effort to get off the open-ended war footing that we've maintained since 9/11. And for these reasons, I indicated in a speech at the National Defense University last May that we needed a more robust public discussion about the balance between security and liberty. Of course, what I did not know at the time is that within weeks of my speech, an avalanche of unauthorized disclosures would spark controversies at home and abroad that have continued to this day.

And given the fact of an open investigation, I'm not going to dwell on Mr. Snowden's actions or his motivations; I will say that our nation's defense depends in part on the fidelity of those entrusted with our nation's secrets. If any individual who objects to government policy can take it into their own hands to publicly disclose classified information, then we will not be able to keep our people safe, or conduct foreign policy. Moreover, the sensational way in which these disclosures have come out has often shed more heat than light, while revealing methods to our adversaries that could impact our operations in ways that we may not fully understand for years to come.

Regardless of how we got here, though, the task before us now is greater than simply repairing the damage done

to our operations or preventing more disclosures from taking place in the future. Instead, we have to make some important decisions about how to protect ourselves and sustain our leadership in the world, while upholding the civil liberties and privacy protections that our ideals and our Constitution require. We need to do so not only because it is right, but because the challenges posed by threats like terrorism and proliferation and cyber-attacks are not going away any time soon. They are going to continue to be a major problem. And for our intelligence community to be effective over the long haul, we must maintain the trust of the American people, and people around the world.

This effort will not be completed overnight, and given the pace of technological change, we shouldn't expect this to be the last time America has this debate. But I want the American people to know that the work has begun. Over the last six months, I created an outside Review Group on Intelligence and Communications Technologies to make recommendations for reform. I consulted with the Privacy and Civil Liberties Oversight Board, created by Congress. I've listened to foreign partners, privacy advocates, and industry leaders. My administration has spent countless hours considering how to approach intelligence in this era of diffuse threats and technological revolution. So before outlining specific changes that I've ordered, let me make a few broad observations that have emerged from this process.

First, everyone who has looked at these problems, including skeptics of existing programs, recognizes that we have real enemies and threats, and that intelligence serves a vital role in confronting them. We cannot prevent terrorist attacks or cyber threats without some capability to penetrate digital communications – whether it's to unravel a terrorist plot; to intercept malware that targets a stock exchange; to make sure air traffic control systems are not compromised; or to ensure that hackers do not empty your bank accounts. We are expected to protect the American people; that requires us to have capabilities in this field.

Moreover, we cannot unilaterally disarm our intelligence agencies. There is a reason why BlackBerrys and iPhones are not allowed in the White House Situation Room. We know that the intelligence services of other countries -- including some who feign surprise over the Snowden disclosures -- are constantly probing our government and private sector networks, and accelerating programs to listen to our conversations, and intercept our emails, and compromise our systems. We know that.

Meanwhile, a number of countries, including some who have loudly criticized the NSA, privately acknowledge that America has special responsibilities as the world's only superpower; that our intelligence capabilities are critical to meeting these responsibilities, and that they themselves have relied on the information we obtain to protect their own people.

Second, just as ardent civil libertarians recognize the need for robust intelligence capabilities, those with responsibilities for our national security readily acknowledge the potential for abuse as intelligence capabilities advance and more and more private information is digitized. After all, the folks at NSA and other intelligence agencies are our neighbors. They're our friends and family. They've got electronic bank and medical records like everybody else. They have kids on Facebook and Instagram, and they know, more than most of us, the vulnerabilities to privacy that exist in a world where transactions are recorded, and emails and text and messages are stored, and even our movements can increasingly be tracked through the GPS on our phones.

Third, there was a recognition by all who participated in these reviews that the challenges to our privacy do not come from government alone. Corporations of all shapes and sizes track what you buy, store and analyze our data, and use it for commercial purposes; that's how those targeted ads pop up on your computer and your smartphone periodically. But all of us understand that the standards for government surveillance must be higher. Given the unique power of the state, it is not enough for leaders to say: Trust us, we won't abuse the data we collect. For history has too many examples when that trust has been breached. Our system of government is built on the premise that our liberty cannot depend on the good intentions of those in power; it depends on the law to constrain those in power.

I make these observations to underscore that the basic values of most Americans when it comes to questions of surveillance and privacy converge a lot more than the crude characterizations that have emerged over the last several months. Those who are troubled by our existing programs are not interested in repeating the tragedy of 9/11, and those who defend these programs are not dismissive of civil liberties.

The challenge is getting the details right, and that is not simple. In fact, during the course of our review, I have often reminded myself I would not be where I am today were it not for the courage of dissidents like Dr. King, who were spied upon by their own government. And as President, a President who looks at intelligence every morning, I also can't help but be reminded that America must be vigilant in the face of threats.

Fortunately, by focusing on facts and specifics rather than speculation and hypotheticals, this review process has given me -- and hopefully the American people -- some clear direction for change. And today, I can announce a series of concrete and substantial reforms that my administration intends to adopt administratively or will seek to codify with Congress.

First, I have approved a new presidential directive for our signals intelligence activities both at home and abroad. This guidance will strengthen executive branch oversight of our intelligence activities. It will ensure that we take into account our security requirements, but also our alliances; our trade and investment relationships, including the concerns of American companies; and our commitment to privacy and basic liberties. And we will review decisions about intelligence priorities and sensitive targets on an annual basis so that our actions are regularly scrutinized by my senior national security team.

Second, we will reform programs and procedures in place to provide greater transparency to our surveillance activities, and fortify the safeguards that protect the privacy of U.S. persons. Since we began this review, including information being released today, we have declassified over 40 opinions and orders of the Foreign Intelligence

Surveillance Court, which provides judicial review of some of our most sensitive intelligence activities -- including the Section 702 program targeting foreign individuals overseas, and the Section 215 telephone metadata program.

And going forward, I'm directing the Director of National Intelligence, in consultation with the Attorney General, to annually review for the purposes of declassification any future opinions of the court with broad privacy implications, and to report to me and to Congress on these efforts. To ensure that the court hears a broader range of privacy perspectives, I am also calling on Congress to authorize the establishment of a panel of advocates from outside government to provide an independent voice in significant cases before the Foreign Intelligence Surveillance Court.

Third, we will provide additional protections for activities conducted under Section 702, which allows the government to intercept the communications of foreign targets overseas who have information that's important for our national security. Specifically, I am asking the Attorney General and DNI to institute reforms that place additional restrictions on government's ability to retain, search, and use in criminal cases communications between Americans and foreign citizens incidentally collected under Section 702.

Fourth, in investigating threats, the FBI also relies on what's called national security letters, which can require companies to provide specific and limited information to the government without disclosing the orders to the subject of the investigation. These are cases in which it's important that the subject of the investigation, such as a possible terrorist or spy, isn't tipped off. But we can and should be more transparent in how government uses this authority.

I have therefore directed the Attorney General to amend how we use national security letters so that this secrecy will not be indefinite, so that it will terminate within a fixed time unless the government demonstrates a real need for further secrecy. We will also enable communications providers to make public more information than ever before about the orders that they have received to provide data to the government.

This brings me to the program that has generated the most controversy these past few months -- the bulk collection of telephone records under Section 215. Let me repeat what I said when this story first broke: This program does not involve the content of phone calls, or the names of people making calls. Instead, it provides a record of phone numbers and the times and lengths of calls -- metadata that can be queried if and when we have a reasonable suspicion that a particular number is linked to a terrorist organization.

Why is this necessary? The program grew out of a desire to address a gap identified after 9/11. One of the 9/11 hijackers -- Khalid al-Mihdhar -- made a phone call from San Diego to a known al Qaeda safe-house in Yemen. NSA saw that call, but it could not see that the call was coming from an individual already in the United States. The telephone metadata program under Section 215 was designed to map the communications of terrorists so we can see who they may be in contact with as quickly as possible. And this capability could also prove valuable in a crisis. For example, if a bomb goes off in one of our cities and law enforcement is racing to determine whether a network is poised to conduct additional attacks, time is of the essence. Being able to quickly review phone connections to assess whether a network exists is critical to that effort.

In sum, the program does not involve the NSA examining the phone records of ordinary Americans. Rather, it consolidates these records into a database that the government can query if it has a specific lead -- a consolidation of phone records that the companies already retained for business purposes. The review group turned up no indication that this database has been intentionally abused. And I believe it is important that the capability that this program is designed to meet is preserved.

Having said that, I believe critics are right to point out that without proper safeguards, this type of program could be used to yield more information about our private lives, and open the door to more intrusive bulk collection programs in the future. They're also right to point out that although the telephone bulk collection program was subject to oversight by the Foreign Intelligence Surveillance Court and has been reauthorized repeatedly by Congress, it has never been subject to vigorous public debate.

For all these reasons, I believe we need a new approach. I am therefore ordering a transition that will end the Section 215 bulk metadata program as it currently exists, and establish a mechanism that preserves the capabilities we need without the government holding this bulk metadata.

This will not be simple. The review group recommended that our current approach be replaced by one in which the providers or a third party retain the bulk records, with government accessing information as needed. Both of these options pose difficult problems. Relying solely on the records of multiple providers, for example, could require companies to alter their procedures in ways that raise new privacy concerns. On the other hand, any third party maintaining a single, consolidated database would be carrying out what is essentially a government function but with more expense, more legal ambiguity, potentially less accountability -- all of which would have a doubtful impact on increasing public confidence that their privacy is being protected.

During the review process, some suggested that we may also be able to preserve the capabilities we need through a combination of existing authorities, better information sharing, and recent technological advances. But more work needs to be done to determine exactly how this system might work.

Because of the challenges involved, I've ordered that the transition away from the existing program will proceed in two steps. Effective immediately, we will only pursue phone calls that are two steps removed from a number associated with a terrorist organization instead of the current three. And I have directed the Attorney General to work with the Foreign Intelligence Surveillance Court so that during this transition period, the database can be queried only after a judicial finding or in the case of a true emergency.

Next, step two, I have instructed the intelligence community and the Attorney General to use this transition period to develop options for a new approach that can match the capabilities and fill the gaps that the Section 215 program was designed to address without the government holding this metadata itself. They will report back to me with options for alternative approaches before the program comes up for reauthorization on March 28th. And during this period, I will consult with the relevant committees in Congress to seek their views, and then seek congressional authorization for the new program as needed.

Now, the reforms I'm proposing today should give the American people greater confidence that their rights are being protected, even as our intelligence and law enforcement agencies maintain the tools they need to keep us safe. And I recognize that there are additional issues that require further debate. For example, some who participated in our review, as well as some members of Congress, would like to see more sweeping reforms to the use of national security letters so that we have to go to a judge each time before issuing these requests. Here, I have concerns that we should not set a standard for terrorism investigations that is higher than those involved in investigating an ordinary crime. But I agree that greater oversight on the use of these letters may be appropriate, and I'm prepared to work with Congress on this issue.

There are also those who would like to see different changes to the FISA Court than the ones I've proposed. On all these issues, I am open to working with Congress to ensure that we build a broad consensus for how to move forward, and I'm confident that we can shape an approach that meets our security needs while upholding the civil liberties of every American.

Let me now turn to the separate set of concerns that have been raised overseas, and focus on America's approach to intelligence collection abroad. As I've indicated, the United States has unique responsibilities when it comes to intelligence collection. Our capabilities help protect not only our nation, but our friends and our allies, as well. But our efforts will only be effective if ordinary citizens in other countries have confidence that the United States respects their privacy, too. And the leaders of our close friends and allies deserve to know that if I want to know what they think about an issue, I'll pick up the phone and call them, rather than turning to surveillance. In other words, just as we balance security and privacy at home, our global leadership demands that we balance our security requirements against our need to maintain the trust and cooperation among people and leaders around the world.

For that reason, the new presidential directive that I've issued today will clearly prescribe what we do, and do not do, when it comes to our overseas surveillance. To begin with, the directive makes clear that the United States only uses signals intelligence for legitimate national security purposes, and not for the purpose of indiscriminately reviewing the emails or phone calls of ordinary folks. I've also made it clear that the United States does not collect intelligence to suppress criticism or dissent, nor do we collect intelligence to disadvantage people on the basis of their ethnicity, or race, or gender, or sexual orientation, or religious beliefs. We do not collect intelligence to provide a competitive advantage to U.S. companies or U.S. commercial sectors.

And in terms of our bulk collection of signals intelligence, U.S. intelligence agencies will only use such data to meet specific security requirements: counterintelligence, counterterrorism, counter-proliferation, cybersecurity, force protection for our troops and our allies, and combating transnational crime, including sanctions evasion.

In this directive, I have taken the unprecedented step of extending certain protections that we have for the American people to people overseas. I've directed the DNI, in consultation with the Attorney General, to develop these safeguards, which will limit the duration that we can hold personal information, while also restricting the use of this information.

The bottom line is that people around the world, regardless of their nationality, should know that the United States is not spying on ordinary people who don't threaten our national security, and that we take their privacy concerns into account in our policies and procedures. This applies to foreign leaders as well. Given the understandable attention that this issue has received, I have made clear to the intelligence community that unless there is a compelling national security purpose, we will not monitor the communications of heads of state and government of our close friends and allies. And I've instructed my national security team, as well as the intelligence community, to work with foreign counterparts to deepen our coordination and cooperation in ways that rebuild trust going forward.

Now let me be clear: Our intelligence agencies will continue to gather information about the intentions of governments -- as opposed to ordinary citizens -- around the world, in the same way that the intelligence services of every other nation does. We will not apologize simply because our services may be more effective. But heads of state and government with whom we work closely, and on whose cooperation we depend, should feel confident that we are treating them as real partners. And the changes I've ordered do just that.

Finally, to make sure that we follow through on all these reforms, I am making some important changes to how our government is organized. The State Department will designate a senior officer to coordinate our diplomacy on issues related to technology and signals intelligence. We will appoint a senior official at the White House to implement the new privacy safeguards that I have announced today. I will devote the resources to centralize and improve the process we use to handle foreign requests for legal assistance, keeping our high standards for privacy while helping foreign partners fight crime and terrorism.

I have also asked my counselor, John Podesta, to lead a comprehensive review of big data and privacy. And this group will consist of government officials who, along with the President's Council of Advisors on Science and Technology, will reach out to privacy experts, technologists and business leaders, and look how the challenges inherent in big data are being confronted by both the public and private sectors; whether we can forge international norms on how to manage this data; and how we can continue to promote the free flow of information in ways that are consistent with both privacy and security.

For ultimately, what's at stake in this debate goes far beyond a few months of headlines, or passing tensions in our foreign policy. When you cut through the noise, what's really at stake is how we remain true to who we are in a world that is remaking itself at dizzying speed. Whether it's the ability of individuals to communicate ideas; to access information that would have once filled every great library in every country in the world; or to forge bonds with people on other sides of the globe, technology is remaking what is possible for individuals, and for institutions, and for the international order. So while the reforms that I have announced will point us in a new direction, I am mindful that more work will be needed in the future.

One thing I'm certain of: This debate will make us stronger. And I also know that in this time of change, the United States of America will have to lead. It may seem sometimes that America is being held to a different standard. And I'll admit the readiness of some to assume the worst motives by our government can be frustrating. No one expects China to have an open debate about their surveillance programs, or Russia to take privacy concerns of citizens in other places into account. But let's remember: We are held to a different standard precisely because we have been at the forefront of defending personal privacy and human dignity.

As the nation that developed the Internet, the world expects us to ensure that the digital revolution works as a tool for individual empowerment, not government control. Having faced down the dangers of totalitarianism and fascism and communism, the world expects us to stand up for the principle that every person has the right to think and write and form relationships freely -- because individual freedom is the wellspring of human progress.

Those values make us who we are. And because of the strength of our own democracy, we should not shy away from high expectations. For more than two centuries, our Constitution has weathered every type of change because we have been willing to defend it, and because we have been willing to question the actions that have been taken in its defense. Today is no different. I believe we can meet high expectations. Together, let us chart a way forward that secures the life of our nation while preserving the liberties that make our nation worth fighting for.

Thank you. God bless you. May God bless the United States of America. (Applause.)

END
11:57 A.M. EST