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;

   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 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.

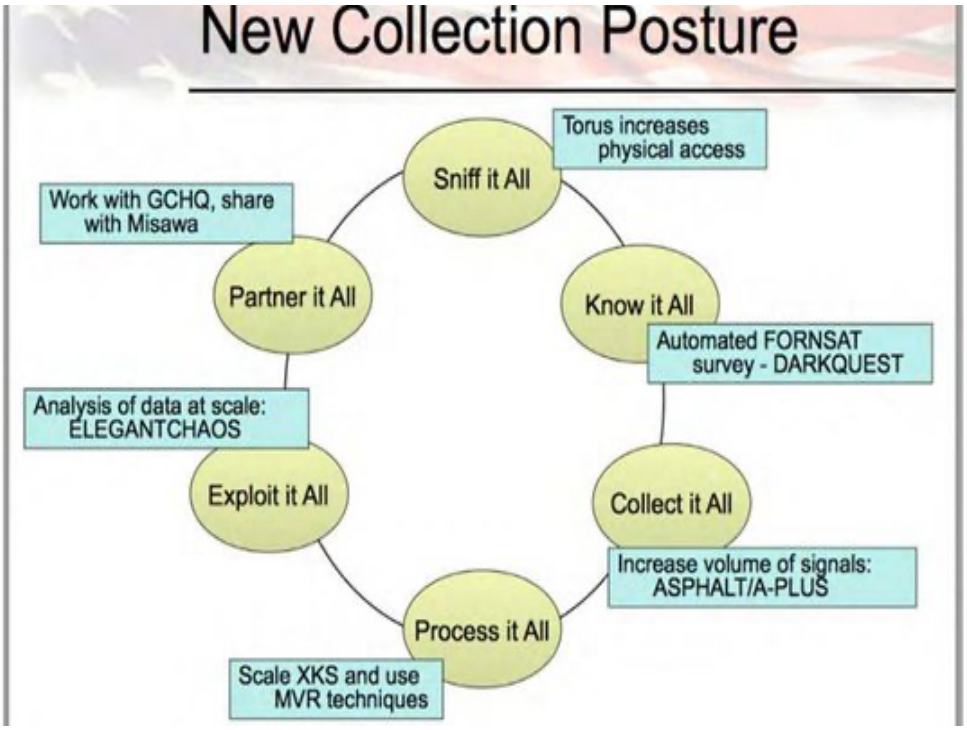
3. There is now produced and shown to me a paginated bundle of true copy documents marked "CC2". All references to documents in this statement are to Bundle CC2 unless otherwise stated, in the form [**CC2/Page**].

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/Page 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.

[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

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

"*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.

[3] http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document

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 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

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

the participation of the providers (Exhibit CC2/Pages x)[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. 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 12333, which I exhibit hereto as [XXX][7].

[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

[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

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' 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[10]. The programs were known as MYSTIC and SOMALGET. This collection, too, was reportedly authorised under E.O. 12,333

    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]

---

[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

[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/

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

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

[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/

exhibit this at [xx]. It shows that pursuant to a single section 702 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 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. **XX**, 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 [XXX]. 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.

Review by oversight bodies

[24] http://scholar.google.com/scholar_case?case=485733189267613105
[25] http://scholar.google.com/scholar_case?case=16871503765334815 48

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: ……..

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