App No. 58170/13

IN THE EUROPEAN COURT OF HUMAN RIGHTS

BETWEEN:

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

Applicants

- v -

UNITED KINGDOM

Respondent

(1) CENTER FOR DEMOCRACY AND TECHNOLOGY
(2) PEN AMERICAN CENTER

Third Party Interveners

JOINT WRITTEN COMMENTS OF THE

THIRD PARTY INTERVENERS

Introduction

1. The Center for Democracy & Technology ('CDT') and PEN American Center ('PEN America') submit these written comments pursuant to leave granted by the President of the First Section under Rule 44 §3 of the Rules of the Court.[1]

2. This Application raises issues of considerable public importance, not only for those residing in the United Kingdom but for a great many people across the Council of Europe, in the context of large-scale secret surveillance undertaken by government agencies and its compatibility with the Convention.

3. Consideration of these issues at the Convention-level cannot ignore the position in the United States:

    a. The Applicants have already adverted to the fact that much of the world's communications flow through the United States; they have also set out the potential scope of the NSA-operated PRISM programme and 'Upstream' activities.[2]

[1] Pursuant to the letter dated 15 December 2015 from the Section Registrar, Søren Nielsen.
[2] Application, II, B, at [18]-[30].

b. Since the filing of the Application, further leaked information has led to suggestions that the government of the United Kingdom has been in receipt of information acquired by US intelligence agencies operating outside of the United States under a regulatory regime distinct from the one that governs PRISM and 'Upstream' acquisition.[3]

c. The extent of the US legal protections for 'non-US persons' subject to surveillance by the United States is relevant to the Court's assessment of the Convention compatibility of the information-sharing arrangements between the United States and the United Kingdom.

4. *Summary of submissions.* By this intervention, CDT and PEN America draw on their expertise, including their particular expertise in the US context, to make the following three submissions to the Court:

(1) The deficiencies in the legal oversight of the United States' regime relating to secret surveillance of non-US targets – deficiencies of which the UK authorities are or ought to be aware – taint the lawfulness of UK intelligence activity such that the criterion of '*in accordance with the law*' is not satisfied under Article 8(2);

(2) The breadth and arbitrary scope of the Unites States' regime ought to be considered by the Court as a factor weighing towards the disproportionality of the surveillance activity under review in this Application; and

(3) The use of secret surveillance on a widespread basis, without sufficient checks and balances, stifles the effective use of the Internet and electronic communication, jeopardizing other Convention rights. The widespread 'chilling effect' upon the exercise of multiple Convention rights requires consideration as part of the Court's proportionality assessment under Article 8(2) in this Application.

5. To assist the Court, these submissions are preceded by a short background section which sets out certain relevant aspects of the surveillance regimes operated by the US intelligence agencies, together with the US legal framework governing those programmes.

Background: The legal regime governing the US intelligence agencies' access to the content of, and information about, communications of 'non-US persons'

6. Where communications surveillance is concerned, the United States draws a distinction between the legal and policy protections that apply to 'US persons'[4] (wherever located) and other persons

[3] Second Witness Statement of Cindy Cohn, 2 March 2015, at [14]-[19].

[4] For the purposes of the relevant US laws and policies, the term 'US person' is defined as '*a citizen of the United States, an alien lawfully admitted for permanent residence…, an unincorporated association a substantial number of members of which*

who are within the United States, on the one hand, and those that apply to non-US persons who are outside of US territory.

7. Surveillance that the NSA conducts within the United States, but that 'targets' foreigners outside of the country, is governed by section 702 of the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 ('FISA'). In particular:

   a. The US Attorney General and the Director of National Intelligence are empowered[5] to authorize the acquisition of 'foreign intelligence information' by targeting non-US persons[6] located outside the United States.[7] 'Foreign intelligence information' is an expansive term that includes, *inter alia*, information that merely '*relates to … the conduct of the foreign affairs of the United States*.'[8]

   b. Section 702 surveillance is purportedly targeted in nature. However, US policy regards 'collection' as occurring (and legal protections as consequently arising) only when a communication is actually selected for examination.[9] Therefore, in the US government's view, the acquisition and/or searching, on an indiscriminate basis, of vast numbers of communications—for example, 'Upstream' surveillance, which entails the monitoring of virtually all Internet traffic that flows over the cables that form the Internet's 'backbone'—does not constitute 'collection' and does not need to be restricted to specific targets.[10]

   c. Although the US authorities must conduct FISA section 702 surveillance in compliance with 'targeting' and 'minimization' procedures that are approved by the Foreign Intelligence Surveillance Court ('FISC'), these procedures are only designed to protect US persons.[11]

   d. The FISC does not review the US government's decision to target any particular person or entity as part of these programmes; it reviews only the government's *procedures* for choosing its targets.[12]

   e. Save where certain criminal prosecutions are involved,[13] there is no statutory provision requiring the US government to provide notification, at any time, to any individual or entity

---

are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States' (50 USC § 1801(i)).

[5] 50 USC § 1881(a); FISA, s702(a).

[6] 50 USC § 1881(a); FISA, s702(b)(3).

[7] 50 USC § 1881(a); FISA, s702(b)(1)-(2).

[8] 50 USC § 1801(e)(2)(B).

[9] See United States Signals Intelligence Directive 18 (USSID SP0018), *Legal Compliance and U.S. Persons Minimization Procedures*, § 9 (Definitions), 25 January 2011.

[10] Ibid.

[11] 50 USC § 1801(h); 50 USC § 1881a(d).

[12] Privacy and Civil Liberties Oversight Board, 'Report on the Surveillance Program Operated Pursuant to Section 702 of the foreign Intelligence Surveillance Act', p. 27 (July 2, 2014).

whose communications have been obtained through section 702 surveillance. This absence of notice, combined with the consistent findings of the US courts that individuals and entities lack standing to challenge section 702 surveillance activities owing to a lack of sufficient proof that they have been monitored,[14] has meant that persons who believe they may have been subjected to unlawful surveillance under this provision have no meaningful avenue of redress.

8. The regulatory framework that applies to US government agencies' acquisition of data and communications when operating outside of the United States is different and even more opaque. It is difficult to be certain as to the precise legal basis of all surveillance programmes conducted by US agencies outside of the jurisdiction, given the secrecy to which such programmes are subject. That said, it is tolerably clear[15] that US agencies operate, or purport to operate, in this context in accordance with Executive Order 12333 ('EO 12333'), issued by President Reagan in 1981 (i.e. without Congressional approval).[16]

9. EO 12333 authorizes, *inter alia*, the collection, retention, and dissemination of *'[i]nformation constituting foreign intelligence or counterintelligence.'*[17] The scope of *'foreign intelligence'* includes not only information relating to the activities of foreign State authorities, but also foreign *'organizations or persons,'*[18] meaning that private individuals come within the scope of the programmes so authorized.

10. Judged against FISA, the powers conferred by EO 12333 are subject to even less oversight. EO 12333 comprises a high-level general authority for bulk and other surveillance of foreign persons outside the United States; but the detailed rules as to its implementation are contained in a series of administrative guidance documents, including Department of Defense Directives 5240.01 and 5240.1-R, and the United States Signals Intelligence Directive USSID SP0018. The Interveners note that substantial portions of that Directive, the Department of Defense Directive 5240.1-R, and the National Security Agency/Central Security Service Policy No. 1 to 23, remain classified and unavailable for public scrutiny.

11. With respect to direct oversight, EO 12333 has not been subject to any mandatory Congressional review or approval. Nor is its use subject to any form of authorization or oversight by the FISC. Further, while President Obama has issued some guidance as to the general principles which US

---

[13] 50 USC § 1806(c), (d). The precise circumstances in which the US government believes it is obligated to provide such notice to defendants remain unclear; see Advocacy for Principled Action in Government et al., Letter to Hon. James R. Clapper, 29 Oct. 2015, pp. 3-4, available at: https://www.brennancenter.org/sites/default/files/analysis/Coalition_Letter_DNI_Clapper_102915.pdf.

[14] See *Wikimedia Foundation, et al v National Security Agency*, US District Court for the District of Maryland, 23 October 2015, pp.17-19; *Clapper v Amnesty Int'l USA*, 133 S. Ct. 1138; 568 U.S. 1 (US Supreme Court), pp.10-15.

[15] Second Witness Statement of Cindy Cohn, 2 March 2015, at [14]-[19].

[16] *United States Intelligence Activities*, Exec. Order No. 12,333, 3 CFR 200 (1981).

[17] See EO 12333, [1.8(a)], [1.11(b)], [1.12(2)(1)], and [1.14(d)].

[18] See EO 12333, [3.4(d)].

agencies should follow in carrying out surveillance of non-US persons in Presidential Policy Directive 28,[19] the guidance is neither binding nor enforceable.

12. A range of surveillance programmes fall under the broad rubric of EO 12333 data and communications acquisition. According to the materials leaked by Edward Snowden, some of these programmes are code-named as follows:

    a. MUSCULAR: a programme under which the US agencies intercept all data transmitted between certain data centres operated by the internet companies Yahoo! and Google outside US territory;

    b. DISHFIRE: a programme under which US agencies intercept private text messages worldwide;

    c. CO-TRAVELLER: a programme under which US agencies intercept location updates from mobile phones worldwide;

    d. MYSTIC: a programme under which US agencies collect all telephone call data in five countries (Mexico, Kenya, the Philippines, the Bahamas, and one undisclosed country), and the entire content of all telephone calls in two of those countries (the Bahamas and the undisclosed country); and

    e. QUANTUM: a programme under which US agencies mount automated attacks (such as the delivery of malware) on Internet users based on certain unknown triggering information.

13. Following the publication by *The Washington Post* of leaked documents in October 2013,[20] it appears that the provision by US intelligence agencies of data and communications to UK government agencies includes information obtained from both FISA section 702 and EO 12333 surveillance.

14. It follows that such information received by the UK government is information the acquisition of which: (a) remains at least partly governed by administrative guidance which is classified; (b) in the case of EO 12333, is not contained in a law that has been subject to transparent Congressional review or public debate; (c) is not the subject of specific judicial authorization or oversight in individual cases; and (d) is, as a practical matter, essentially incapable of being effectively challenged in the US courts by affected persons.

---

[19] *Signals Intelligence Activities*, PPD-28 (2014).

[20] Barton Gellman and Ashkan Soltani, 'NSA Infiltrates Links to Yahoo, Google data centers worldwide, Snowden documents say,' *The Washington Post* (30 October 2013), available at: 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

<u>Submission 1</u>: The deficiencies in the US legal regime render UK government activity in breach of the 'in accordance with the law' criterion of Article 8(2)

15. The Interveners respectfully submit that, were the authority for a UK policy not fully accessible to the public, only partly subject to Parliamentary scrutiny, and outside the scope of effective judicial oversight, this Court could be expected to decide that, insofar as the policy interfered with qualified Convention rights, that interference would fail to satisfy the threshold criterion of being 'in accordance with the law,' in the sense of it not being set out in domestic law in a manner which is accessible, sufficiently certain, and provides protection against its arbitrary application.

16. This Court's recent statement in the case of ***Szabó and Vissy v Hungary*** (a successful challenge to Hungarian legislation on secret anti-terrorist surveillance) is of direct relevance and application in this case:[21]

> "where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident [and it] is therefore essential to have clear, detailed rules on interception [which are] sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to such measures."

Where the detailed rules governing surveillance remain classified such that the persons potentially subject to it are unable to gain any, or any adequate, indication of the powers of the executive and the conditions upon which those powers may, or may not be, exercised, the Interveners submit that the relevant interference with qualified Convention rights cannot properly be described as accessible or certain.

17. The Interveners further note this Court's view that, in the field of state surveillance *'control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exception, warranting close scrutiny.'*[22] Surveillance activities undertaken pursuant to EO 12333 are done so without any independent oversight, while those undertaken pursuant to FISA section 702 are carried out without any specific judicial scrutiny of individual cases.

18. The UN Human Rights Committee has expressed clear concern about the inadequacies of the legal safeguards that apply to secret surveillance programmes conducted by the NSA:[23]

> 'The Committee is concerned about the surveillance of communications in the interest of protecting national security, conducted by the [NSA] both within and outside the United States … in particular, [through] surveillance under Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendment Act,

[21] *Szabó and Vissy v Hungary*, Application No. 37138/14, Judgment of 12 January 2016, at [62].
[22] *Szabó and Vissy v Hungary*, Application No. 37138/14, Judgment of 12 January 2016, at [77].
[23] U.N. Doc. CCPR/USA/CO/4 (Apr. 23, 2014), ¶22 *et seq.* Available here: http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2FC%2FUSA%2FCO%2F4

> conducted through PRISM (collection of communications content from United States-based Internet companies) and UPSTREAM (collection of communications metadata and content by tapping fiber-optic cables carrying Internet traffic) and the adverse impact on individuals' right to privacy. The Committee is concerned that, until recently, judicial interpretations of FISA and rulings of the Foreign Intelligence Surveillance Court (FISC) had largely been kept secret, thus not allowing affected persons to know the law with sufficient precision. The Committee is concerned that the current oversight system of the activities of the NSA fails to effectively protect the rights of the persons affected. While welcoming the recent Presidential Policy Directive/PPD-28, which now extends some safeguards to non-United States citizens "*to the maximum extent feasible consistent with the national security*", the Committee remains concerned that such persons enjoy only limited protection against excessive surveillance…'

19. The Interveners submit that, if the regimes of data and communications collection for which section 702 and/or EO 12333 provide would themselves fail the test of being *'in accordance with the law'* for the purposes of Article 8(2) of the Convention, it should follow that the UK government's regulatory framework must also fail the same test, on the basis that it allows for the receipt of such data and communications pursuant to that US legal regime. This deficiency – whereby UK agencies are tainted by the deficiency of the US framework under which data and communications were originally obtained – is separate to, and independent of, the direct deficiencies identified by the Applicants with respect to the inadequate regulation of the process by which UK agencies receive data and communications from their US counterparts.[24]

20. Further, if the Applicants are correct to contend that there is no framework governing the United Kingdom's disclosure of information to the United States,[25] then it should follow that there is no satisfactory safeguard against abuse by the United States on receipt of the information. Therefore, the surveillance and information sharing programmes between the two states are in breach of the '*in accordance with the law*' criterion under Article 8(2).

<u>Submission 2</u>: The deficiencies in the US legal regime render UK government activity in breach of the proportionality principle under Article 8(2)

21. The Interveners respectfully submit that, were this Court to be asked to consider the compatibility of the surveillance programmes conducted pursuant to section 702 and EO 12333 with the Convention, it could be expected to determine that interferences with Article 8 rights arising under those programmes were disproportionate under Article 8(2).

22. The Court is invited to note that in the context of large-scale internet and communications surveillance regimes of a type similar to those at issue in this case, the UN High Commissioner for Human Rights has specifically warned that *'[m]andatory third party data retention – a recurring*

[24] See Application, at [119]-[139].
[25] See Applicants' Updated Submission, at [59]; see also Application, at [39]-[40].

feature of surveillance regimes in many States, where Governments require telephone companies and Internet service providers to store metadata about their customers' communications and location for subsequent law enforcement and intelligence agency access – appears neither necessary nor proportionate.'[26]

23. Certain programmes operated under EO 12333 and section 702 display precisely that defect of universal collection. Under the MUSCULAR programme, for instance, all data flowing into certain Yahoo! and Google facilities is acquired, without any discrimination as to its nature, source, or content. Similarly, under the MYSTIC programme, all telephone call details are collected in five countries, and the entire contents of telephone calls are collected in two such countries. Nor is the breadth of such programmes an aberration: on the contrary, it is entirely consistent with the breadth of authority granted by EO 12333, and within the scope of the powers the US authorities consider section 702 to grant.

24. In circumstances where it is clear that the surveillance programmes operated under EO 12333 and section 702 would themselves be judged disproportionate, by virtue of their broad interferences with privacy at the bulk level without any particular targeting, the Interveners submit that the UK government's actions, in cooperating with and participating in those same programmes, are implicated in the same disproportionality under Article 8(2).

<u>Submission 3</u>: The wider impact of bulk surveillance on the proportionality analysis

25. In conducting its proportionality assessment, the Court ought to afford particular significance to the right to privacy. This is because it is only through the possession of a protected zone of privacy that individuals are able fully to enjoy other human rights, including the right to hold opinions and the right to freedom of expression. Successive U.N. Special Rapporteurs on the Promotion and Protection of the Right to Freedom of Opinion and Expression have, in recent reports, endorsed the right to privacy as the *'gateway to the enjoyment of other rights,'*[27] and strongly endorsed principles of online privacy protection, such as encryption and anonymity, as consistent with human rights protection.[28]

26. Where individuals lack confidence in the privacy of their electronic communications and Internet use, their willingness freely to express their opinions, and to seek and to impart information – activities essential in any democratic system of government – is fettered by means of self-censorship. In particular:

---

[26] Report of the Office of the UN High Commissioner for Human Right, *The Right to Privacy in the Digital Age*, UN Doc. A/HRC/27/37 (2014), at [26].

[27] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc. A/HRC/29/32 (2015) ('Kaye Report'), at [16]. See also UN General Assembly, Resolution 68/187 *The Right to Privacy in the Digital Age*, UN Doc. A/RES/68/167 (2014), Recitals.

[28] Kaye Report, at [16]-[18]. See also Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc. A/HRC/23/40 (2013) ('La Rue Report'), at [81]-[90].

a. The Special Rapporteurs for Freedom of Expression for the U.N. and Inter-American Commission on Human Rights have issued a joint declaration on surveillance programmes and their impact on freedom of expression, expressing concern that the surveillance programmes operated by the United States '*could severely affect the right to freedom of thought and expression and the right to privacy*'.[29] Further, the Special Rapporteurs stressed the need to place limits on surveillance programmes and observed that while '*the Internet has created unprecedented opportunities for the free expression, communication, possession, search for, and exchange of information*', this has resulted in '*police and security forces running surveillance programmes intended to combat terrorism and defend national security [...] without adequate regulation in the majority of the states in our region*'.[30]

b. The U.N. Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression has acknowledged that '*privacy and freedom of expression are interlinked and mutually dependent; an infringement upon one can be both the cause and consequence of an infringement upon the other. Without adequate legislation and legal standards to ensure the privacy, security and anonymity of communications, journalists, human rights defenders and whistle-blowers, for example, cannot be assured that their communications will not be subject to the States' scrutiny*'.[31]

c. This Court has held time and again that journalists, whistle-blowers and human rights defenders are the guardians of any rights-protecting democracy and that restrictions upon them will harm the values which the Convention seeks to protect.[32] Further, of course, where the communications of those persons sit within particular contexts, such as the context of confidential communications between accused persons and their lawyers, surveillance of those communications (as has recently been revealed to occur in the UK)[33] may constitute an infringement of rights other than privacy, such as the Article 6 right of confidential communication as an aspect of effective legal assistance and a fair trial.[34]

---

[29] United Nations Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights: *Joint Declaration on Surveillance Programmes and their Impact on Freedom of Expression*, 21 June 2012. Available at: http://www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1

[30] Ibid, at [4].

[31] Ibid, at [79].

[32] See *MGN v UK*, Application No 39401/04, Judgment of 18 January 2011, at [141]; *Flux v Moldova*, Application No 28702/03, Judgment of 12 November 2007, at [43]; *Castells v Spain*, Application No 11798/85, Judgment of 23 April 1992, at [43]; *Thorgeir Thorgeirson v Iceland*, Application No 13778/88, Judgment of 25 June 1992, at [63]; *Jersild v Denmark*, Application No 15890/8, Judgment of 23 September 1994, at [31].

[33] *Belhadj and ors v The Security Service and ors*, IPT/13/132-9/H, Judgment of 29 April 2015.

[34] *Moiseyev v Russia*, Application No 62936/00, Judgment of 9 October 2008, at [202]ff. For an assessment of the practical impact of surveillance on attorney-client relationships in the United States, see: Human Rights Watch, *With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy* (2014), available at: https://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and

27. Therefore, a proportionality assessment of the interference with the Applicants' Article 8 rights in this case must take into account of not only the direct impact of surveillance on privacy rights but also the indirect, but no less significant, 'chilling effect' that surveillance has on the willingness of writers, journalists, publishers, human rights defenders and others to communicate with sources, share information, and fearlessly publish in the exercise of the right to freedom of expression. It also must take into account the chilling effect on the enjoyment of free expression and similar rights by ordinary citizens, and the resulting impact on democracy.

28. The Interveners wish to draw this Court's attention to two substantial surveys of writers, journalists, and media professionals conducted by PEN America, the results of which demonstrate that, following the revelation in mid-2013 of widespread state surveillance programmes such as those to which the present Application relates, writers have self-censored their work in multiple ways, including through reluctance to address certain subjects and reluctance to communicate with sources or colleagues for fear of endangering those individuals through their being identified to government authorities.[35]

29. Strikingly, the research conducted for PEN's 2015 report revealed that more than 1 in 3 writers in 'free' countries (including the United Kingdom) said that they had avoided writing or speaking on a particular topic, or had seriously considered it, due to concerns about surveillance.[36] In the four countries other than the United States which make up the "Five Eyes" surveillance alliance (Australia, Canada, New Zealand and the United Kingdom) 84% of writers surveyed reported that they were very or somewhat worried about government surveillance.[37]

HUGH SOUTHEY Q.C.
Matrix Chambers

CAN YEGINSU
ANTHONY JONES
4 New Square Chambers

SARAH ST.VINCENT
Center for Democracy & Technology
1401 K Street NW, Floor 2
Washington, DC 20005.

KATHERINE G. BASS
Pen American Center
588 Broadway, Suite 303
New York, NY 10012.

[35] See PEN America, *Chilling Effects: NSA Surveillance Drives US Writers to Self-Censor* (2013); see also PEN America, *Global Chilling: The Impact of Mass Surveillance on International Writers* (2015) ('*Global Chilling*'), available at: http://www.pen-international.org/wp-content/uploads/2015/01/Global-Chilling_01-05-15_FINAL.pdf

[36] PEN America, *Global Chilling*, p.10.

[37] Ibid, p.7.