App No. 62322/14

IN THE EUROPEAN COURT OF HUMAN RIGHTS

BETWEEN:

(1) BUREAU OF INVESTIGATIVE JOURNALISTS

(2) ALICE ROSS

Applicants

-and-

THE UNITED KINGDOM

Respondent

WRITTEN COMMENTS OF THE CENTER FOR DEMOCRACY AND TECHNOLOGY

Introduction

1. The Center for Democracy and Technology ('CDT') submits these written comments pursuant to the permission granted by the President of the First Section on 15 December 2015, under Rule 44 §3 of the Rules of the Court.

2. CDT is a civil society organization devoted to defending global online civil liberties and human rights. CDT is based in Washington, DC and has a presence in Brussels and London. CDT is dedicated to keeping the Internet open, innovative, and free, and is committed to finding solutions to the most pressing challenges facing users of electronic communications technologies. Since its founding, CDT has played a leading role in shaping the policies, practices, and norms that have empowered individuals to use these technologies effectively as speakers, entrepreneurs, and active citizens. In addition, CDT has intervened in numerous landmark cases relating to Internet-related human rights and media freedoms, including before this Court in the recent case of ***Szabó and Vissy v. Hungary***[1] and the application currently before this Court in ***Big Brother Watch and others v. United Kingdom***.[2]

---

1 *Szabó and Vissy v. Hungary*, Application No. 37138/14, Judgment of 12 January 2016.
2 *Big Brother Watch and others v. United Kingdom*, Application No. 58170/13.

3. This Application raises issues of considerable public importance which touch on the freedoms of residents of the United Kingdom and many other people, within Council of Europe States and beyond, whose Internet communications have a connection with the United Kingdom. As the Applicants have noted, the United Kingdom's Government Communications Headquarters ('GCHQ'), in its surveillance programmes, collaborates with the authorities of the United State of America and receives intelligence gathered by the US National Security Agency ('NSA').[3] Accordingly, the lawfulness of the programmes under which the NSA gathers such intelligence is itself of direct relevance to the lawfulness of the UK's surveillance regime.

4. This Application concerns large-scale surveillance programmes in the United Kingdom and United States. The applicants, the Bureau of Investigative Journalism (BIJ) and Alice Ross, a reporter with the BIJ, suspect that their Convention right to privacy under Article 8 and to freedom of expression under Article 10 have been violated as a result of these programmes, and that this has undermined their roles as *'public watchdog[s]'*.[4]

5. *Summary of submissions*. Mindful of the need to avoid duplicating the submissions already made by the Applicants and the other third party interveners, CDT draws on its expertise with respect to the situation of Internet surveillance in the United States to make the following two submissions to this Court:

   (1) The governing rules of the US regime relating to secret surveillance of non-US targets are not sufficiently transparent and are open to arbitrary application, such that the US regime, and the UK regime which relies upon intelligence provided by the US regime, fails to satisfy the criteria that interference with human rights must be *'in accordance with the law'* under Article 8(2) and *'prescribed by law'* under Article 10(2) of the Convention; and

   (2) The breadth and arbitrary scope of the United States regime ought to be considered by this Court as a factor weighing towards the disproportionality of the surveillance regime challenged in the Application.

6. 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

---

[3] See Application, at [36]-[37].

[4] See Application, at [122].

intelligence agencies, together with the US legal framework governing those programmes.

Background

7. In the United States, surveillance of communications is governed by significantly different regimes depending upon whether the target of the surveillance is: (a) a *'US person'*[5] (wherever located) and other persons who are within the US; or (b) a non-US person outside US territory.

Section 702 of the Foreign Intelligence Surveillance Act

8. Where the NSA conducts surveillance *from within* the US, but which targets non-US persons outside US territory, such activity is governed by section 702 of the Foreign Intelligence Surveillance Act ('FISA'). This surveillance involves the compelled disclosure, both from storage and in real time, by US companies of communications content, traffic data and subscriber information of persons reasonably believed to be outside the US. In particular:

   a. The US Attorney General and the Director of National Intelligence are empowered[6] to authorize the acquisition of *'foreign intelligence information'* by targeting non-US persons[7] located outside the United States. *'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, according to US policy, *'collection'* (which is subject to certain legal restrictions) only occurs 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 a vast volume of communications – for example, the UPSTREAM surveillance programme, which entails the monitoring, by the NSA or by compelled US

---

5 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 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).

6 50 USC § 1881(a); FISA, s702(a).

7 50 USC § 1881(a); FISA, s702(b)(3).

8 50 USC § 1801(e)(2)(B).

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

communications service providers, of virtually all Internet traffic that flows over the cables forming the Internet's 'backbone'[10] – does *not* constitute *'collection'* and so does not need to be restricted to specific targets.

c. Although US authorities must conduct FISA section 702 surveillance in compliance with *'targeting'* and *'minimization'* procedures approved by the Foreign Intelligence Surveillance Court ('FISC'), these procedures are mainly designed to protect US persons and persons inside the US, and not non-US persons located outside the US.[11]

d. The FISC does not review the US government's decision to target any particular person or entity under its surveillance programmes; the FISC only reviews the government's *procedures* for choosing 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 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.

Executive Order 12333

9. The legal framework applying to US government agencies' collection of data and communications conducted *outside* the US 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

---

10 As noted in the Application, at [35]; Privacy and Civil Liberties Oversight Board, supra, at pp. 36-37; Julia Angwin, 'AT&T Helped U.S. Spy on Internet on a Vast Scale,' *New York Times* (15 August 2015), available at: http://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html?_r=1.

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

12 Privacy and Civil Liberties Oversight Board, supra, at p.27.

13 50 USC § 1806(c), (d).

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.

programmes are subject. That said, it is tolerably clear[15] that US agencies operate, or purport to operate, in accordance with Executive Order 12333 ('EO 12333'), issued by President Reagan in 1981 (i.e. without Congressional approval) outside of the US.[16]

10. EO 12333 authorizes, among other things, the collection, retention, and dissemination of *'[i]nformation constituting foreign intelligence or counterintelligence*.'[17] The scope of *'foreign intelligence*' for these purposes 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 programmes so authorized.

11. Most of the rules governing the implementation of EO 12333 are not available to the public. Detailed rules for 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. CDT notes that substantial portions of USSID SP0018 remain classified, and that information, as well as many official interpretations of the DoD Directives, are unavailable for public scrutiny. CDT further notes that interpretations of these directives remain classified. President Obama has, in Presidential Policy Directive 28,[19] issued some guidance as to the general principles which US agencies should follow in carrying out surveillance of non-US persons. However, PPD-28 is neither binding nor enforceable, and the rules governing its implementation are only publicly available in part.

12. Judged against FISA, the powers conferred by EO 12333 are subject to even less independent oversight. Specific EO 12333 queries or investigations are not subject to judicial authorization, nor is there any oversight of them by the FISC. EO 12333 has never been subject to mandatory Congressional review or approval. And while the Privacy and Civil Liberties Oversight Board, an independent executive agency, has the authority to review EO 12333 activities, it has not yet produced its first report on the Order.

13. By virtue of their secret nature, the scope of the surveillance programmes purportedly operated under EO 12333 is not entirely clear. However, according to the materials

---

15 See Amos Toh et al, *Overseas Surveillance in an Interconnected World*, Brennan Center for Justice (2016).

16 *United States Intelligence Activities*, Exec. Order No. 12333, 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)].

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

leaked by Edward Snowden relating to NSA activities, some of the code-named programmes conducted are as follows:

a. MUSCULAR: a programme under which 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 domestic and international telephone call data, and much communications content, in five countries (Mexico, Kenya, the Philippines, the Bahamas, and one other country – potentially Iraq[20] or Afghanistan);[21] and

e. QUANTUM: a programme under which US agencies mount automated attacks (such as the delivery of computer malware) on Internet users based on certain unknown triggering information.[22]

14. It follows that the data and communications received by the UK government from the US intelligence agencies 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 a transparent legislative process; (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.

---

[20] According to a statement by former NSA Deputy Director John C Inglis, reported in Glenn Greenwald, 'NSW Blows Its Own Top Secret Program in Order to Propagandize,' *The Intercept* (31 March 2014), available at: https://theintercept.com/2014/03/31/nsa-worlds-blows-top-secret-program/.

[21] According to analysis by Wikileaks. See: Julian Assange, 'Wikileaks Statement on the Mass Recording of Afghan Telephone Calls by the NSA,' *Wikileaks* (23 May 2014), available at: https://wikileaks.org/WikiLeaks-statement-on-the-mass.html.

[22] See Sarah St.Vincent and Joe Hall, *Five US Surveillance Programs Undermining Global Human Rights* (18 September 2014), available at: https://cdt.org/blog/five-us-surveillance-programs-undermining-global-human-rights/.

<u>Submission 1</u>: The governing rules of the US regime relating to secret surveillance of non-US targets are not sufficiently transparent and are open to arbitrary application, such that the US regime, and the UK regime which relies upon intelligence provided by the US regime, fails to satisfy the criteria that interference with human rights must be *'in accordance with the law'* under Article 8(2) and *'prescribed by law'* under Article 10(2) of the Convention.

15. CDT respectfully submits 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: [23]

> 'especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. 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 the US surveillance regimes under section 702 of FISA and/or EO 12333 remain classified, with the result that the persons potentially subject to that surveillance 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, CDT submits that the relevant interference with qualified Convention rights is not taking place pursuant to a legal framework which can properly be described as accessible or certain.

17. CDT further notes 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*

---

[23] *Szabó and Vissy*, at [62].

substitute solutions the exception, warranting close scrutiny.'[24] 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 surveillance targets.

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, including those relevant to this Application:[25]

> '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 [amendments to] the Foreign Intelligence Surveillance Act (FISA) Amendment Act, 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 national security", the Committee remains concerned that such persons enjoy only limited protection against excessive surveillance...'

19. If the programmes of data and communications collection for which the US legal regime provides would themselves fail the test of being *'in accordance with the law'* or *'prescribed by law'* for the purposes of Articles 8(2) and 10(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 the flawed US legal regime.

---

24 *Szabó and Vissy*, at [77].

25 UN Human Rights Committee, Concluding Observations on the Fourth Periodic Report of the United States of America, UN Doc. CCPR/C/USA/CO/4 (2014), at [22].

<u>Submission 2</u>: The deficiencies of the US legal regime render UK government activity in breach of the proportionality principle under Article 8(2) and Article 10(2) of the Convention.

20. CDT submits that, were this Court to be asked to consider the compatibility of the surveillance programmes conducted by US agencies pursuant to section 702 and EO 12333 with the Convention, it could be expected to determine that interferences with Article 8 and Article 10 rights arising under those programmes were disproportionate under Articles 8(2) and 10(2) respectively.

21. 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 feature of surveillance regimes in many States, where Government 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]

22. Certain activities carried out by US agencies pursuant to EO 12333 and section 702 display precisely that defect of universal collection. For instance:

    a. Under the MUSCULAR programme, all data flowing into certain Yahoo! and Google facilities is acquired, without any discrimination as to its nature, source, or content.

    b. Under the MYSTIC programme, the NSA engages in indiscriminate collection of telephone call details in the counties to which it applies.

23. 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 the rights to privacy and freedom of expression at the bulk level without any particular targeting, CDT submits that the UK government's actions, in cooperating with and participating in those same programmes, are implicated in the same disproportionality under Articles 8(2) and 10(2) of the Convention.

---

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

HUGH SOUTHEY Q.C.
Matrix Chambers

CAN YEGINSU
ANTHONY JONES
4 New Square Chambers

7 July 2016

CHRISTINE GALVAGNA
Center for Democracy & Technology
1401 K Street NW
Suite 200
Washington, DC 20005.