App Nos. 58170/13, 62322/14, 24960/15

BEFORE THE GRAND CHAMBER
OF THE EUROPEAN COURT OF HUMAN RIGHTS

BETWEEN:

BIG BROTHER WATCH AND ORS

Applicants

-v-

THE UNITED KINGDOM

Respondent

CENTER FOR DEMOCRACY AND TECHNOLOGY

Third-Party Intervener

WRITTEN COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY

Introduction

1. The Center for Democracy & Technology ('**CDT**') submits these supplementary written comments pursuant to leave granted by the President of the Grand Chamber under Rule 44 § 5 of the Rules of the Court.[1]

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

3. Any consideration of that issue must take into account the fact that member States, in their bulk communications and metadata surveillance activities, co-operate with, and rely upon, the government of the United States to a greater or lesser extent. That is the case not only because much of the world's digital communications flows through the United States, but also because certain member States operate specific information-sharing programmes with the U.S. intelligence agencies, themselves operating both

[1] Pursuant to the letter dated 3 April 2019 from the Deputy Grand Chamber Registrar, Søren Prebensen. CDT previously submitted written comments as a third-party intervener in the applications in *Big Brother Watch and others v The United Kingdom* (App No. 58170/13) and *Bureau of Investigative Journalists and Alice Ross v United Kingdom* (App No. 62322/14).

within and outside U.S. territory. As a result, the extent of U.S. legal protections for 'non-U.S. persons' subject to surveillance by U.S. agencies is relevant to this Court's assessment of the Convention compatibility of the surveillance regimes operated by member States.

4. CDT seeks to rely in full on its written comments in App. Nos. 58170/13 and 62322/14, as submitted to, and considered by, the First Section.[2] In these supplementary written comments, CDT draws on its expertise to make the following two renewed submissions to this Court:

   4.1. The U.S. regime relating to secret surveillance of non-U.S. targets is lacking in necessary safeguards such that any surveillance activity carried out by member States which involves information sharing with the U.S. intelligence agencies fails to satisfy the criterion of lawfulness under Article 8(2) or Article 10(2) of the Convention; and

   4.2. In the event that this Court determines that the bulk surveillance programmes at issue in these Applications are lawful *in principle*, this Court is invited to provide guidance as to the necessary elements of Convention-compliant oversight regimes where international cooperation is involved.

Submission 1: Lawfulness under Article 8(2) and Article 10(2)

5. There are two separate regimes under U.S. law that govern data and communications surveillance of non-U.S. nationals: one which applies when U.S. agencies operating from within the United States target non-U.S. nationals located outside the U.S.; and a second regime which applies when U.S. agencies are themselves operating outside U.S. territory.

Surveillance from within the U.S. of overseas foreign nationals

6. Surveillance from within the U.S. directed at foreign targets is governed by section 702 of the Foreign Intelligence Surveillance Act of 1978 ('**FISA**').[3] That section, added to FISA in 2008, provides for the *'targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information,'* subject to the joint authority

[2] This Court's attention is drawn, in particular, to the short background sections in both sets of written comments, setting out certain relevant aspects of the surveillance regimes operated by the U.S. intelligence agencies, together with the U.S. legal framework governing those programmes, see [6]-[14] in the *Big Brother* third-party intervention, and [7]-[14] in the *Alice Ross* third-party intervention.

[3] Now reflected in the US Code as: 50 USC § 1881a.

of the Attorney General and the Director of National Intelligence.[4] The definition of *'foreign intelligence information'* is broad and covers all information which *'relates to … the conduct of the foreign affairs of the United States.'*[5] Surveillance authorized under this FISA regime is required to comply with 'targeting' and 'minimization' procedures approved by the Foreign Intelligence Surveillance Court ('**FISC**'). However, that system of purported oversight is, in practice, substantially constrained:

6.1. First, such 'targeting' and 'minimization' procedures are only designed to protect U.S. persons;[6]

6.2. Secondly, the FISC does not review decisions to target any particular person or entity; the scope of its review is limited to oversight of the government's *procedures* for choosing targets;[7]

6.3. Thirdly, the regulatory regime, as a matter of U.S. policy, only applies where the intelligence agencies undertake the activity of *actually selecting a communication for examination*.[8] Accordingly, the prior stages of automatic or 'passive' acquisition and/or monitoring of communications and data – such as through the 'UPSTREAM' programme, which entails the monitoring of virtually all internet traffic which flows through the internet cabling infrastructure in US territory – do not come within the regulatory regime and do not need to be restricted to specific authorized targets;[9] and

6.4. Fourthly, save in certain exceptional cases where criminal prosecutions are involved, there is no statutory requirement upon agencies 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 such surveillance activities without specific

---

4 50 USC § 1881a(a).
5 50 USC § 1801(e).
6 50 USC § 1801(h); 50 USC § 1881a(d).
7 See: Privacy and Civil Liberties Oversight Board, 'Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act' (2 July 2014), p27.
8 See: United States Signals Intelligence Directive 18 (USSID SP0018), *Legal Compliance and US Persons Minimization Procedures* (25 January 2011), § 9 (Definitions).
9 The UPSTREAM programme was suspended in 2017 for failure to comply with rules regarding protection of U.S. persons. In reauthorizing Section 702 in 2018, the U.S. Congress permitted the NSA to resume UPSTREAM collection with notice to Congress that the collection problem had been addressed; see Section 103 of the FISA Amendments Reauthorization Act, Pub. L. no. 115-118, January 19, 2018.

proof they have been monitored,[10] means that individuals who believe they may have been subject to unlawful surveillance have no meaningful redress.

Surveillance outside the U.S. of foreign nationals

7. The regulatory framework which applies to U.S. government agencies' acquisition of data and communications when operating *outside* U.S. territory is different and even more opaque. Given the secrecy to which programmes conducted by U.S. agencies overseas are subject, it is difficult to be certain what authority such agencies purport to act under, but it is generally understood that U.S. intelligence agencies rely upon Executive Order 12333 (as amended) ('**EO 12333**'), an executive order originally issued, without Congressional approval, by President Reagan in 1981.[11] Since then, subsequent Presidents have reaffirmed EO12333, with President Obama in January 2017 releasing a set of procedures for EO12333 activities as they relate to 'raw' signals intelligence information,[12] the effect of which was to allow intelligence agencies to share that raw information with all the U.S. government's 16 intelligence agencies for analysis.[13]

8. EO12333 authorizes, *inter alia*, the collection, retention, and dissemination of *'[i]nformation constituting foreign intelligence or counterintelligence.'*[14] The scope of *'foreign intelligence'* includes not only information relating to the activities of foreign State authorities, but also foreign *'organizations or persons,'*[15] meaning that private individuals come within the scope of its operations. Operations under EO12333 are subject to even less oversight than those under the FISA regime: activities carried out purportedly under its authority are not subject to oversight by the FISC, and much of the detailed operational framework is set out in government guidance (including the Department of Defense Directives 5240.01 and 5240.1-R, and National Security Agency/Central

---

[10] *Clapper v Amnesty Int'l USA*, 133 S Ct 1138 US 1 (US Supreme Court), pp10-15.

[11] *United States Intelligence Activities*, Exec. Order No. 12333, 3 CFR 200 (1981), as amended by *Strengthened Management of the Intelligence Community*, Exec. Order No. 13355, 69 FR 53593 (2004) and *Further Amendments to Executive Order 12333, United States Intelligence Activities*, Exec. Order 13470, 73 FR 45325 (2008).

[12] Presidential Policy Directive – Signals Intelligence Activities (PPD-28), 12 January 2017, https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

[13] See: C Savage, 'NSA Gets More Latitude to Share Intercepted Communications,' *The New York Times* (12 January 2017), available at: https://www.nytimes.com/2017/01/12/us/politics/nsa-gets-more-latitude-to-share-intercepted-communications.html.

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

[15] EO 12333, § 3.4(d).

Security Service Policy Nos. 1 to 23) which are not subject to judicial review or Congressional authorisation.

9. On the basis of the materials leaked by Edward Snowden, it appears that the U.S. intelligence agencies purportedly rely upon EO12333 as the basis for a series of data and communications acquisition programmes including those under the following code names:

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

   9.2. DISHFIRE: A programme under which U.S. agencies intercept private text messages worldwide;

   9.3. CO-TRAVELLER: A programme under which U.S. agencies intercept location updates from mobile phones worldwide;

   9.4. MYSTIC: A programme under which U.S. agencies collect all telephone call data in five countries (Mexico, Kenya, the Philippines, the Bahamas, and one other country – potentially Iraq[16] or Afghanistan),[17] and the entire content of all telephone calls in two of those countries (the Bahamas and the undisclosed country); and

   9.5. QUANTUM: A programme under which U.S. agencies mount automated attacks (such as the delivery of malware) on internet users outside U.S. territory based on certain unknown triggering information.

10. There has been no indication from the U.S. government that any of these programmes first revealed in 2013 have been abandoned.

11. It follows that the data and communications received by the U.K. government from U.S. intelligence agencies is information the acquisition of which: (a) remains at least partly governed by administrative guidance the contents of which is classified and

[16] According to a statement by former NSA Deputy Director John C Inglis, reported in G Greenwald, 'NSA 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/.

[17] 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.

unknown to the public or this Court; (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 authorisation or oversight in individual cases; and (d) is, as a practical matter, essentially incapable of being effectively challenged in the U.S. courts by affected persons.

12. This Court has consistently held 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.'*[18] CDT notes, however, that, in its decisions in the *Big Brother and ors v. United Kingdom* and *Bureau of Investigative Journalists and Alice Ross v United Kingdom* applications, the First Section has taken the view that while prior judicial authorisation may be a '*best practice*,' it is not absolutely required if alternative *'checks and balances'* (such as the existence of non-judicial but nonetheless independent oversight institutions) provided adequate safeguards for the interception regime as a whole.[19] But even adopting that broad view of the U.S. regime governing foreign data and communications interception, that regime falls well below the required standard for independent oversight as a result of: (a) the absence of legislative scrutiny of the enabling rules; (b) the absence of prior judicial oversight for the vast majority of operations not subject to the FISC; and (c) the absence of effective *ex post* judicial review given that individuals do not have standing to bring challenges to court without the very evidence of their surveillance which is kept secret.

13. CDT submits that, since the regime of data and communications collection for which the U.S. regime provides under Section 702 of FISA and/or EO 12333 would itself fail to satisfy the minimum criterion of lawfulness for the purposes of Article 8(2) or Article 10(2) of the Convention, it should follow that member States' regulatory frameworks must also fail the same test insofar as they allow for the receipt of such data and communications through cooperation with the U.S. intelligence agencies.

<u>Submission 2</u>: Guidance as to the necessary elements of Convention-compliant oversight regimes where international cooperation is involved

14. While CDT's position is that bulk surveillance activities are by their very nature disproportionate and therefore unlawful under the Convention, it recognizes that the

[18] *Szabó and Vissy v Hungary* [2016] ECHR 579; (2016) 63 EHRR 3, at [77].
[19] *Big Brother Watch and ors v United Kingdom* [2018] ECHR 722, at [318]-[320].

First Section, giving judgment in respect of the *Big Brother Watch* and *Bureau of Investigative Journalists and Alice Ross* Applications, held that bulk data and communications interception regimes were not in principle unlawful, noting that such regimes fall within the state's margin of appreciation *'in choosing how best to achieve the legitimate aim of protecting national security.'*[20] In doing so, the First Section confirmed the view taken more than a decade ago in the admissibility decision in *Weber and Saravia v Germany*[21] and the judgment in *Liberty and ors v United Kingdom*,[22] when the question of the compatibility of bulk communications interception with the Convention was first considered.

15. In the event that this Court similarly takes the view that bulk data and communications interception activities are not *per se* unlawful under the Convention, CDT respectfully submits that this Court ought to take the present opportunity to set out clear guidance as to the necessary elements of a Convention-compliant oversight regime, mindful that, as the First Section held, *'all interception regimes (both bulk and targeted) have the potential to be abused, especially where the true breadth of the authorities' discretion to intercept cannot be discerned from the relevant legislation.'*[23]

16. CDT submits that the circumstances of international cooperation in bulk data and communications surveillance require that at least three conditions are met: (a) that states must actively assess and satisfy themselves as to the adequacy of their foreign partners' legal and administrative framework governing interception, and set out these adequacy measures in domestic law; (b) that there must be independent – preferably judicial – authorisation, based on a finding of reasonable suspicion, for the use of selectors[24] identifiable to specific targets to query information obtained from foreign partners or from a member States' own bulk surveillance; and (c) that there must be a requirement of subsequent notification to the subjects of interception measures, including internationally.

---

20 *Big Brother Watch*, at [314].

21 *Weber and Saravia v Germany*, App No 54934/00 (Decision of 29 June 2006), at [137].

22 *Liberty and ors v United Kingdom* [2008] ECHR 568; (2009) 48 EHRR 1. In *Liberty*, the Fourth Section proceeded on the basis that the bulk interception of telephone, fax, and email communications was capable of operation in a lawful manner, but, as a matter of fact, constituted a breach of Article 8 because UK domestic law did not *'indicat[e] with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications'* and *'was not, therefore, "in accordance with the law"'* (at, [69]).

23 *Big Brother Watch*, at [315].

24 As indicated in the First Section's judgment in *Big Brother Watch*, a "selector" is a specific identifier, such as an email address, relating to a known target [12].

17. With respect to member States' review of their foreign partners, the criteria that the foreign partner's law and practice must meet should be established by law.[25] Current state practice within the Council of Europe provides examples of how such mechanisms can be implemented at the domestic level:[26]

    17.1. In the Netherlands, the Act on the Intelligence and Security Services 2017 requires that the Dutch intelligence services, in order to determine with which foreign intelligence agencies there may be cooperation in respect of data and communications interception, must first draw up a 'weighting note' on that foreign partner, and submit that note for review by the independent Review Committee on Intelligence and Security.[27] The 'weighting notes' must address the five issues of: (a) the democratic oversight of the intelligence and security services in the country concerned; (b) the respect for human rights in the country concerned; (c) the professionalism and reliability of the service concerned; (d) the legal powers and capabilities of the service in the country concerned; and (e) the level of data protection maintained by the service concerned; and

    17.2. In Germany, Section 13 of the Federal Intelligence Service Law requires that all cooperation agreements involving bulk signals intelligence with foreign states require prior written authorisation by way of Memorandum of Understanding and approval from the Chancellery.[28]

18. With respect to requiring a judicial finding of reasonable suspicion for use of a selector identifiable to a particular surveillance target, CDT submits that such a requirement merely reflects, at the level of international transfers of information, the same safeguard which this Court has consistently imposed[29] upon the exercise of member States' own surveillance powers. The First Section in *Big Brother Watch* dismissed the suggestion of requiring a finding of reasonable suspicion in relation to persons for whom data is

---

[25] This would be in keeping with, in the context of information sharing with a foreign partner, the First Section's caution in *Big Brother Watch* that, "… *the circumstances in which intercept material can be requested from foreign intelligence services must also be set out in domestic law in order to avoid abuses of power*", at [424].

[26] For a survey of current international practice with respect to bulk surveillance generally, see: T Wetzling and K Vieth, 'Upping the Ante on Bulk Surveillance: An International Compendium of Good Legal Safeguards and Oversight Innovations' (Heinrich Böll Stiftung Publication Series on Democracy, Vol 50, 8 November 2018), available at: https://www.stiftung-nv.de/sites/default/files/upping_the_ante_on_bulk_surveillance_v2.pdf.

[27] Act on the Intelligence and Security Services 2017, Articles 88-90.

[28] BND Law, Section 13.

[29] See *Zakharov v Russia* [2015] ECHR 1065; (2016) 63 EHRR 17, at [258]; and *Szabó*, at [77]-[79].

sought as "*inconsistent…with the operation of a bulk interception regime.*"[30] However, such a requirement can be a safeguard imposed after interception has already occurred, and before security agencies in member States review information about a specific target. Therefore a judicial finding of reasonable suspicion is not "*impossible*"[31] in this context.

19. The requirement of some form of independent authorisation – judicial or otherwise – by which security agencies are required to justify the grounds upon which they seek to exercise their powers in relation to personal data, has become a general principle of human rights law, recognized under EU law also. In the joined cases *Tele2* and *Watson and ors,*[32] the CJEU reiterated that access by national authorities to retained data *'should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body.'*[33] The rationale for requiring security agencies to justify their need to exercise powers before an independent body is self-evident. In the words of the Council of Europe Human Rights Commissioner, *'the security agency has to go "outside of itself" and convince an independent person of the need for a particular measure. It subordinates security concerns to the law, and as such it serves to institutionalize respect for the law. If it works properly, judicial authorisation will have a preventive effect, deterring unmeritorious applications …'* [34] The need for intelligence agencies to justify the querying of information obtained from foreign partners is just as pressing as with purely domestic requests. For that reason, this Court is invited to make clear that the requirement of prior judicial authorisation for the use of a particular selector to query data applies as much to information obtained through international intelligence sharing arrangements as they do in the domestic context.

20. Further, CDT submits that any Convention-compliant system of surveillance which involves sharing of information from data and communications interception internationally must satisfy the additional condition that the persons subjected to such interception are provided with subsequent notification of that fact, so that they may, if they have grounds, challenge the lawfulness of that interception before courts of competent jurisdiction. This Court has specified as much in its judgment in the *Szabó*

---

30 *Big Brother Watch*, at [317].
31 *Big Brother Watch*, at [317].
32 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Postoch telestyrelsen* and *Secretary of State for the Home Department v Watson, Brice, and Lewis* ECLI:EU:C:2016:970.
33 *Tele2*, [120]. See also Case C-293/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* ECLI:EU:C:2014:238, [62].
34 Council of Europe Human Rights Commissioner, *Memorandum on Surveillance and Oversight Mechanisms in the United Kingdom* (Comm DH (2016)20, May 2016), [28].

and Vissy case, which itself cited the position of the 2013 report of the United Nations Special Rapporteur on the promotion and protection of the right to freedom of expression.[35] The First Section in *Big Brother Watch* assumed that notice was incompatible with the operation of a bulk interception regime.[36] Notice to all subject to bulk interception can be achieved by a requirement that the relevant bulk interception programme be publicly-acknowledged and described with particularity sufficient to give notice of the type of information that can be collected and the breadth of the collection effort. In addition, there must also be particularized notice to: (i) any person against whom the information collected will be used in a criminal investigation; and (ii) any person whose selector was run against the information collected in bulk, provided that such notice can be delayed if it would undermine the purpose of the surveillance.

21. As the situation in the United States demonstrates, if there is no obligation upon state agencies to provide positive notification to persons who have been subject to surveillance, persons who suspect that they have been so targeted may be left without the necessary evidence to bring any form of proceedings for review of the lawfulness of such measures, frustrating their access to any effective remedy. CDT submits that, at the very least, persons whose selectors are used to query data, and persons accused of crimes based on such surveillance are due subsequent notification so that they may have access to redress if necessary, and that condition should apply equally in cases of international cooperation regarding intelligence sharing as it clearly does when state surveillance activities are restricted within states' territories.

CAN YEGINSU
ANTHONY JONES
4 New Square Chambers,
4, New Square, Lincoln's Inn,
London, WC2A 3RJ.

24 April 2019

GREGORY T. NOJEIM
Center for Democracy & Technology
1401 K Street NW, Suite 200
Washington, D.C. 20005

---

[35] '*Individuals should have a legal right to be notified that they have been subjected to communications surveillance or that their communications data has been accessed by the State. Recognizing that advance or concurrent notification might jeopardize the effectiveness of the surveillance, individuals should nevertheless be notified once surveillance has been completed and have the possibility to seek redress in respect of the use of communications surveillance measures in their aftermath.*: see 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 (17 April 2013), at [82], cited in *Szabó and Vissy*, at [24].

[36] *Big Brother Watch*, at [317].