IN THE EUROPEAN COURT OF HUMAN RIGHTS **App No. 24960/15**

10 HUMAN RIGHTS ORGANIZATIONS AND OTHERS

– v –

THE UNITED KINGDOM

THIRD PARTY INTERVENTION OF THE ELECTRONIC PRIVACY INFORMATION CENTER

---

1. The Electronic Privacy Information Center ("EPIC") welcomes the opportunity to submit these written comments. EPIC was granted leave to intervene on February 26, 2016, by the President of the First Section under Rule 44 § 3 of the Rules of the Court. EPIC filed written submissions in the proceedings before the Chamber and has chosen to make fresh submissions in these proceedings before the Grand Chamber.
2. EPIC is a leading privacy and freedom of information organization in the United States. EPIC was established in 1994 to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age.[1] EPIC pursues a wide range of program activities including policy research, public education, conferences, litigation, publications, and advocacy. EPIC also works closely with a distinguished board of advisors, who are experts in law, technology and public policy and maintains one of the most popular privacy web sites in the world—epic.org. EPIC has participated as amicus curiae in close to one hundred cases in the United States and as third-party intervener with the European Court of Human Right in *Privacy International and Others v. the United Kingdom* (App No. 46259/16).[2]
3. The matter before the Court in *10 Human Rights Organizations and Others v. the United Kingdom* implicates important human rights including privacy, data protection and freedom of expression. This case is among the first in which the Grand Chamber will consider the lawfulness of "bulk" surveillance. It is also the first to examine compatibility of an intelligence transfer arrangement with the Convention.
4. EPIC respectfully urges the Court to consider the scope of U.S. surveillance capabilities in reviewing compliance of UK surveillance authorities and also to consider U.S.-UK intelligence transfers within the European Convention on Human Rights. When communications data is gathered under terms below Convention standards, transfer of that data to a Party circumvents the Convention's guarantees. As EPIC's intervention explains, first, that U.S. law authorizes mass, indiscriminate surveillance of non-U.S. persons located outside the U.S., and, second, that U.S. surveillance practices violate the Convention because they do not provide the requisite Article 8 safeguards.

---

[1] *See* EPIC, *About EPIC*, EPIC.org, https://epic.org/epic/about.html.
[2] *See* EPIC, *EPIC Amicus Curiae Briefs*, EPIC.org, https://epic.org/amicus/.

Communications intelligence transferred from the U.S. to the UK are necessarily colored by this underlying violation.

I. U.S. law authorizes mass, indiscriminate foreign surveillance

5. The U.S. intelligence community is authorized by law and presidential order to engage in foreign surveillance without individualized suspicion, prior judicial authorization, or notice, and for generalized purposes divorced from national security. In particular, legal authorities grant practically unfettered discretion to acquire data concerning non-U.S. persons located abroad.

6. Foreign surveillance by U.S. agencies is governed by three primary legal authorities. First, an act of Congress, Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act, governs surveillance targeting foreign communications collected on U.S. soil for national security purposes. Surveillance of non-U.S. persons executed abroad is not governed by any act of Congress but is instead carried out under Presidential authority pursuant to Executive Order 12333. Finally, Presidential Policy Directive 28 (PPD-28), issued by President Obama in 2014, placed certain limitations on surveillance of non-U.S. persons. These rules do not introduce meaningful limits, particularly as to the *collection* of foreign persons' data, and PPD-28 can be rescinded or modified by the President at any time without notice. The U.S. can order Communications Service Providers to produce stored data via mandatory directive or compel a company to provide facilitate interception of communications data as it transits fiber optic cables ("bearers").

FISA Section 702

7. The FISA was enacted in 1978 "to provide a statutory procedure for the authorization of applications for a court order approving the use of electronic surveillance to obtain foreign intelligence information."[3] In 2008 the U.S. Congress amended the FISA to include "Section 702." Surveillance under Section 702 takes place in the United States with the compelled assistance of communications service providers in the U.S. but targets non-U.S. persons "*reasonably believed to be located outside the United States*."[4] Two of the surveillance programs at issue in this case, "Prism" and "Upstream," are carried out pursuant to Section 702.

8. There is no prior judicial review of surveillance activity, no individualized suspicion required, no review of whether any particular target is an agent of a foreign power or engaged in criminal activity, nor does the government have to specify to a court the specific facilities or places at which electronic surveillance is to be directed. Instead, under Section 702, the U.S. Attorney General and the Director of National Intelligence jointly authorize on an annual basis a "program" of surveillance—ongoing surveillance which must be carried out according to a set of procedures that are subject to an annual review.

9. These U.S. officials are empowered to jointly authorize surveillance that (1) targets non-United States persons, (2) who are reasonably believed to be located outside the United States, (3) with the compelled assistance of an electronic communication service

[3] Foreign Intelligence Surveillance Act of 1978, S. Rep. 95-604, pt. 1, at 3, reprinted in 1978 U.S.C.C.A.N. 3904, 3905 (1978).

[4] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, §702, 122 Stat. 2436, 2438-2448 (2008) (codified at 50 U.S.C. § 1881a).

provider, (4) in order to acquire foreign intelligence information.[5] The government acquires communications under Section 702 by compelling the assistance of communications providers—including data processors and internet backbone telecommunications providers.[6]

10. The Foreign Intelligence Surveillance Court ("FISC") annually reviews the "*targeting*" and "*minimization*" procedures for Section 702 surveillance as well as the certifications of the Attorney General and the Director of National Intelligence, and confirms the procedures' compliance with the statutory requirements.[7] The targeting procedures must be "*reasonably designed*" to ensure collection is limited to targeting persons reasonably believed to be outside of the U.S. and prevent "*intentional*" collection of entirely domestic communications.[8] The minimization procedures must be "*reasonably designed*" to minimize the acquisition and retention, and prohibit the dissemination, of U.S. persons' information.[9] Following the annual approval by the FISC, the U.S. Government is authorized to acquire foreign communications without individual judicial oversight.

11. Section 702 surveillance may be conducted for purposes other than national security. First, gathering of "*foreign intelligence information*" need only be a "*significant purpose*" of data collection, meaning that collection may also be for other purposes.[10] Further, "*foreign intelligence information*" is defined broadly in five categories related to foreign attack; terrorism; proliferation of weapons of mass destruction, but also "*the conduct of the foreign affairs of the United States*."[11]

12. There is no statutory obligation to notify subjects of Section 702 surveillance. The statute solely requires the government to provide notice where it uses Section 702 information against an individual in proceedings, such a criminal defendant.[12]

13. Section 702 provides practically unfettered discretion to acquire the communications of non-U.S. persons abroad. The statutory restrictions on acquisition Section 702 are all designed to prevent surveillance of Americans and individuals located in the United States.[13] As described above, the Attorney General, in consultation with the Director of National Intelligence must also adopt both targeting and minimization procedures.[14] The targeting and minimization procedures in Section 702 are likewise designed to provide protections for Americans and persons located in the U.S. The Section 702 targeting procedures must be "*reasonably designed*" to limit acquisition to targets reasonably believed to be located outside the United States and to prevent the acquisition of purely domestic communications.[15] And the minimization procedures must satisfy a four-part

---

[5] 50 U.S.C. § 1881a(a)
[6] Ibid. § 1881a(i)(A).
[7] Ibid. § 1881a(a).
[8] Ibid. § 1881a(d).
[9] Ibid. § 1881a(e).
[10] Ibid. § 1881a(h)(2)(A)(v).
[11] 50 U.S.C. § 1801(e).
[12] 50 U.S.C. § 1806(c—d). *But see* Human Rights Watch, Dark Side: Secret Origins of Evidence in US Criminal Cases (2018), https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases ("controversies continue as to whether the government is complying fully with its obligation to notify defendants of surveillance" under Section 702).
[13] 50 U.S.C. § 1881a(b)(1)—(5).
[14] Ibid. § 1881a (d)(1), (e)(1).
[15] Ibid. § 1881a(d).

definition centered around the minimization of acquisition, retention, and dissemination of Americans' information.[16] Simply put, none of the surveillance restrictions in Section 702 provide any protection for non-U.S. persons abroad.

EO 12333

14. The U.S. Intelligence Community ("USIC") conducts surveillance outside of the United States pursuant to Presidential authority pursuant to Executive Order 12333.[17] First issued in 1981, the Order establishes a framework for the activities of the USIC, including the collection of signals intelligence. EO 12333 is the primary source of authority for the National Security Agency ("NSA") programs to acquire foreign intelligence.[18] And surveillance conducted pursuant to EO 12333 is not subject to public law nor public scrutiny. There are no reports or official disclosures concerning the scope of surveillance under EO 12333.

15. The Order provides broad authority to conduct signals intelligence surveillance. The USIC is authorized under EO 12333 to collect signals intelligence from a wide variety of sources, including data transiting fiber optic networks. In contrast to Section 702, collection under EO 12333 occurs outside of U.S. territory. For example, EO 12333 would include acquisition of "*data from the deep underwater cables on the floor of the Atlantic by means of which data are transferred from the EU to the US for processing within the US before the data arrives within the US*."[19]

16. Under EO 12333, signals intelligence may be conducted to gather "*foreign intelligence and counterintelligence*."[20] Foreign intelligence is more broadly defined than under the FISA, and includes "*information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists*."[21]

17. There is no judicial oversight of signals intelligence collection carried out pursuant to EO 12333— not even annual programmatic review of procedures, as is for Section 702 surveillance. EO 12333 likewise places no specific limits on the duration of surveillance, nor does it require notification to subjects of surveillance.

18. The authorization for collection of information concerning non-U.S. persons under EO 12333 provides virtually unfettered discretion. EO 12333 limits the collection, retention, and dissemination of "*information concerning United States persons*" by requiring that Intelligence Community agencies adopt procedures to limit collection of information to

---

[16] Ibid. § 1881a(e). Minimization procedures are further defined in 50 U.S.C. §§ 1801(h), 1821(4).

[17] Exec. Order No. 12,333: 40 Fed. Reg. 59,941 (Dec. 4, 1981), reprinted as amended in 73 Fed. Reg. 45,328 (2008) (July 30, 2008).

[18] *Data Protection Commissioner v. Facebook Ireland and Schrems,* Irish High Court, McGovern J., Judgment of 3rd October 2017, § 175, https://www.dataprotection.ie/sites/default/files/uploads/2018-12/High%20Court%20Judgment_03_10_2017.pdf [hereinafter Irish "Schrems II" Judgment]. The Irish High Court made extensive findings of fact regarding U.S. surveillance based on the testimony of experts. The judgment is one of the few publicly available, authoritative documents describing elements of EO 12333.

[19] Irish "Schrems II" Judgment, § 176.

[20] Ibid. § 3.5(f).

[21] EO 12333 § 3.5(e).

enumerated categories.[22] The Order imposes a general restriction on collection by requiring that members of the USIC use *"the least intrusive collection techniques feasible within the United States or directed against United States persons abroad*" and stating the Intelligence community is not authorized to engage in electronic surveillance except "*in accordance with procedures"* establish by high level officials.[23]

PPD-28

19. Presidential Policy Directive 28 (PPD-28) is a 2014 presidential order imposing certain restrictions on U.S. signals intelligence activities that implicate personal information regardless of the nationality or location of the person.[24] Importantly, PPD- 28 does not limit the discretion of the U.S. intelligence community to collect non-U.S. persons' data, and expressly permits "*bulk*" surveillance.

20. PPD-28 outlines four "*principles*", framed as general limitations on all signals intelligence collection by the U.S. Government.[25] The first principle requires that collection "*be authorized*" by law or executive order and undertaken in a lawful manner.[26] The second principle states that *"[p]rivacy and civil liberties shall be integral considerations*" in the planning of signals intelligence activities and prohibits collection for specified improper purposes.[27] The third principle prohibits the "*collection of foreign private commercial information or trade secrets*" in order to "*afford a competitive advantage to U.S. companies.*"[28] And the fourth and final principle requires that collection "*be as tailored as feasible*."[29]

21. PPD-28 also addresses signals intelligence collected in "*bulk*." PPD-28 defines "*bulk collection*" as: "*the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.).*"[30] The Directive expressly notes that bulk collection can "*result in the collection of information about persons whose activities are not of foreign intelligence or counterintelligence value.*"[31] PPD-28 limits the use of communications acquired in bulk but does not prohibit bulk collection. The directive merely requires that the U.S. limit use of non-publicly available signals intelligence collected in "*bulk*" to six listed purposes.[32] The modest limitations on "*bulk*" surveillance are also subject to an exception: they "*do not apply to signals intelligence data that is temporarily acquired to facilitate targeted collection*."[33]

II. U.S. surveillance violates Article 8, at a minimum, for the failure to limit the scope of application and duration, and the failure to provide adequate supervision, notice, and remedies

---

[22] Ibid. § 2.3.
[23] Ibid. § 2.4.
[24] WHITE HOUSE, PRESIDENTIAL POLICY DIRECTIVE 28: SIGNALS INTELLIGENCE ACTIVITIES (2014) [hereinafter PPD-28].
[25] PPD-28 § 1(a)—(d).
[26] Ibid. § 1(a).
[27] Ibid. § 1(b).
[28] Ibid. § 1(c).
[29] Ibid. § 1(d).
[30] Ibid. § 2.
[31] Ibid. § 2 n.5.
[32] Ibid. § 2.
[33] Ibid. § 2 n.5.

22. The U.S. framework for foreign surveillance violates Article 8, necessarily coloring any transfer of data to the U.K. While exhaustive review of U.S. surveillance is impossible within the constraints of a third-party intervention, such an exhaustive review is unnecessary because of clear shortcomings as compared against Article 8 requirements. U.S. surveillance violates Article 8, at a minimum, for the overbroad scope of application and duration of surveillance, as well as inadequate supervision, notice, and remedies for Section 702 and EO 12333 collection activities.

23. Article 8 of the Convention requires state interferences with the right to privacy only be insofar as is "*in accordance with the law*" and "*necessary in a democratic society*" in pursuit of a legitimate aim.[34] "*In accordance with law*" requires surveillance have both a sufficient basis in domestic law and, second, compatibility with the rule of law (interpreted to mean both accessible and foreseeable in effects).[35] As to "*necessity*," in *Szabó and Vissy v. Hungary* and *Klass and Others v. Germany Klass and Others v. Germany* this Court emphasized interception regimes are permissible only insofar as "*strictly necessary*" to satisfy legitimate aims. [36]

24. The "*Weber* criteria," used to gauge foreseeability, are a cornerstone of the caselaw on secret surveillance. These mandatory minimum transparency safeguards must be provided by law to "*avoid abuse of power*" in interception for criminal investigations and national security. The law must make clear:

    - Scope - The nature of offences which may give rise to an interception order, and the definition of the categories of people liable to have their communications intercepted
    - A limit on the duration of interception
    - The procedure to be followed for examining, using and storing the data obtained
    - The precautions to be taken when communicating the data to other parties
    - The circumstances in which intercepted data may or must be erased or destroyed.[37]

    Any arrangements for supervising implementation of secret surveillance measures, notification mechanisms and remedies provided for by national law will also be considered.[38] Surveillance should be subject to prior judicial or other independent authorization and subjects should receive "*subsequent notification of surveillance measures*" because notice is "*inextricably linked to the effectiveness of remedies*."[39]

Scope

25. Current U.S. statutes and presidential orders fail to appropriately limit the scope of surveillance—both as to the nature of the offenses for which individuals may be subject to surveillance and the categories of people affected. As a result, there is not an

---

[34] European Convention on Human Rights art. 8, Nov. 4, 1950, ETS No. 005; *Liberty v. United Kingdom*, App. No. 58243/00, Eur. Ct. H.R., Judgment, 26 (2008);
[35] *Roman Zakharov v. Russia* [GC], no. 47143/06, § 228., ECHR 2015.
[36] *Szabó and Vissy v. Hungary*, No. 37138/14, § 54, ECHR 2016; *Klass and Others v. Germany Klass and Others v. Germany*, 6 September 1978, § 42., Series A no. 28
[37] *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 95 ECHR 2006-X
[38] *Szabó*, §§ 75—88.
[39] *Zakharov,* § 171; *Szabó*, § 86.

"*adequate indication as to the circumstances in which public authorities are empowered to resort to such measures*."[40]

26. The nature of the offenses for which U.S. surveillance can be authorized are generalized, divorced from any specific national security justification, and provide substantial discretion to authorities to conduct surveillance.

27. In *Case of Kennedy v. United Kingdom* the Court deemed general terms like "*serious crime*" and "*national security*" sufficiently tailored because they were further defined by policy and law.[41] The purposes for which U.S. surveillance can be conducted are not similarly tailored. The U.S. wields nearly unfettered discretion in deciding what predicate acts can justify surveillance of non-U.S. persons abroad. For example, as discussed above, under Section 702 only a "*significant purpose*" of the collection must be to gather "*foreign intelligence information*"—granting broad discretion to authorities to order surveillance for other purposes.[42] "*Foreign intelligence information*" is also itself broadly defined to include the "*foreign affairs*" of the U.S.[43] This term is not further defined in the statute or in USIC procedures for conducting Section 702 surveillance.[44]

28. Similarly, under EO 12333, the USIC is authorized to collect "*intelligence and counterintelligence*,"[45] where foreign intelligence includes "*information relating to the capabilities, intentions, or activities of*" both "*foreign organizations*" and "*foreign persons*."[46] Also not further defined, these terms, unlike those in 702, are arguably self-evident or capable of definition against other fully specified terms, such as "*U.S. person.*" Yet by the same token, the terms are so general in nature that they fail to cabin the circumstances under which surveillance can be issued and against whom.

29. The U.S. framework for surveillance also does not sufficiently identify the categories of people affected by surveillance. In *Szabó*, the Court concluded that "*sufficient reasons for intercepting a specific individual's communications [should] exist in each case*."[47] By contrast, in *Liberty and Others v. the United Kingdom*, the Court concluded that U.K. law authorizing interception of non-domestic communications violated Article 8 where "*extremely broad discretion*" was granted to intercept external communications and to the selection of communications for examination, and where the procedures for examining and utilizing data were not public.[48] U.S. surveillance is a close analog.

---

[40] *Zakharov*, § 243
[41] *Kennedy*, § 159.
[42] 50 U.S.C. § 1801a(h)(2)(A)(v).
[43] 50 U.S.C. § 1801(e).
[44] *See generally* 50 U.S.C. 1801; Nat'l Sec. Agency, PPD-28 Section 4 Procedures (2015); Nat'l Sec. Agency, USSID SP0018 Legal Compliance and U.S. Persons Minimization Procedures (2011); Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended (2017); Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978 (2017).
[45] EO 12333 § 3.5(f).
[46] Ibid. § 3.5(e).
[47] *Szabó*, § 73.
[48] *Liberty and Others v. the United Kingdom*, no. 58243/00, §§ 64—70, 1 July 2008.

30. As discussed above, under FISA Section 702, review by the FISC is limited to approval of the annual Section 702 certifications. Neither 702 nor EO 12333 involve the establishment of "probable cause," any individualized review of whether any particular target is engaged in criminal activity, or the identification of specific facilities at which electronic surveillance is to be directed. There is also no requirement to justify the proportionality of the surveillance in relation to the aim.

31. As described in detail above, none of the limitations on collection under EO 12333 or FISA 702 protect non-U.S. persons, leaving collection virtually unrestrained by statute or order aside from generalized limitations such as the requirement in PPD-28 that surveillance "*be as tailored as feasible*."[49]

32. In practice, the PPD-28 requirement can mean capturing communications of an entire "region." The USIC procedures state that whenever practicable, under PPD-28's requirement a "*selector*"—an identifier like a telephone number or e-mail address associated with targeted individuals—will be used.[50] However, the Director of National Intelligence has explained that where no specific selector associated with a group is know the U.S. "*might choose to target that group by collecting communications to and from that region for further review and analysis to identify those communications that relate to the group*."[51]

Duration

33. As to duration**,** the Court reiterated in *Zakharov v. Russia* that surveillance may be left "*to the discretion of the relevant domestic authorities which have competence to issue and renew interception warrants*," but only insofar as *"adequate safeguards exist, such as a clear indication in the domestic law of the period after which an interception warrant will expire, the conditions under which a warrant can be renewed and the circumstances in which it must be cancelled*."[52] However, U.S. foreign surveillance can theoretically have unlimited duration.

34. EO 12333 places no limits on the duration of surveillance conducted under its authority. Because there are no requirements for the government to seek a surveillance order or undergo court review, surveillance can in theory continue indefinitely.

35. Meanwhile, surveillance under Section 702 is functionally unlimited. As described in detail above, 702 surveillance includes an annual programmatic review by the FISC of the surveillance procedures. Approval of the 702 surveillance program by FISC is standard, and, as a result, the program of surveillance has continued uninterrupted since its inception.[53]

---

[49] PPD-28 § 1(d).
[50] Ibid. § 4.2.
[51] Letter from Office of the Gen. Counsel to the Office of Dir. of Nat'l Intelligence to Counselor Dep't of Commerce Justin Antonipillai & Ted Dean Deputy Assistant Sec'y Int'l Trade Admin. (June 21, 2016), https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q1A.
[52] *Zakharov*, § 250.
[53] *See, e.g.*, Office of the Dir. of Nat'l Intelligence, Statistical Transparency Report Regarding Use of National Security Authorities: Calendar Year 2017 13 (2018), https://www.dni.gov/files/documents/icotr/2018-ASTR----CY2017----FINAL-for-Release-5.4.18.pdf (listing one 702 order issued annually since reporting was initiated in 2013, except

36. PPD-28 did not introduce any limits on the duration of EO 12333 or 702 surveillance.

Supervision, notification, and remedies

37. Finally, the U.S. framework for foreign surveillance fails to include the necessary supervision, notice, and remedies.

38. U.S. surveillance law does not require judicial authorization foreign surveillance. The importance of judicial authorization as a safeguard for secret surveillance is a key principle under Article 8. At the stages when surveillance is authorized or being carried out, because of the inherent risk of abuse, it is desirable to entrust "*supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure*."[54] Yet, as detailed above, FISA Section 702 eschews individualized judicial review of surveillance orders with an annual "programmatic" review of the procedures for carrying out surveillance. Surveillance activities under EO 12333 are not subject to any judicial oversight.

39. In *Kennedy*, the Court carved out a narrow exception to the requirement for judicial authorization. Broad jurisdiction to hear claims regardless of the complainants' notice of surveillance can, in some instances, compensate for the lack of individualized judicial oversight of surveillance.[55] In that case, Court looked favorably on the United Kingdom system, in which any person who thinks that he or she has been subject to secret surveillance can lodge a complaint with the IPT.[56] The same is true in the United States, and the lack of judicial control of surveillance fatally falls short of Article 8's requirements.

40. The "standing doctrine" significantly restrict redress in privacy and surveillance cases in the U.S. The Constitutional jurisdiction of federal courts has been interpreted to require plaintiffs to demonstrate an "injury-in-fact" that is "actual or imminent," "concrete," and "particularized."[57] This rule requires that any individual seeking redress for surveillance prove (1) an injury, (2) a causal connection between the injury and government conduct, and (3) a likelihood that the injury will be redressed by a favorable decision.[58]

41. In a pivotal case challenging Section 702, *Clapper v. Amnesty Int'l USA*, the U.S. Supreme Court held that a group of U.S. citizen plaintiffs did not have standing to challenge the surveillance program.[59] The plaintiffs, a group of attorneys, advocates, and others who routinely communicated with foreigners abroad, contended there was an objectively reasonably likelihood that their communications would be collected under Section 702, and that they suffered a present harm from surveillance because they undertook burdensome measures to protect the confidentiality of their communications.[60] The Court concluded the plaintiffs' claim must fail both because it

---

in 2016 "when the 2015 order remained in effect" during extended FISC review of the certifications).

[54] *Zakharov*, § 233.

[55] *Kennedy v. United Kingdom*, no. 26839/05, § 167, 18 May 2010.

[56] Ibid.

[57] U.S. CONST. art. III, § 2.

[58] *Lujan v. Defenders of Wildlife*, 504 U. S. 555, 560—61 (1992) (citations omitted).

[59] *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1145 (2013).

[60] Ibid. 133 S. Ct. at 1143.

was "*too speculative*" and because plaintiffs could not prove surveillance would occur under Section 702 as opposed to another legal authority for surveillance.[61]

42. Under *Clapper*, an individual will likely not be able to sustain a legal challenge to surveillance without specific evidence that he or she was the subject of surveillance and confirmation of the specific statutory authority used by the United States. As described above, there is no general statutory obligation in the U.S. to notify subjects of surveillance, except when the government introduces evidence in a formal criminal proceeding.[62] Because individuals are unlikely to receive notice of Section 702 or EO 12333 surveillance, a claim arising from surveillance is likely to fail the *Clapper* test and individuals will not be able to seek redress even for unlawful surveillance.
43. Finally, without any obligation to notify those affected by surveillance the vast majority of individuals will not have any way to know that they have a reason to seek redress. As this Court has emphasized, "*There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively*."[63] In short, the failure to notify subjects of surveillance compromises any available remedies.

III. Conclusion

44. EPIC submits that U.S. law authorizes mass, indiscriminate surveillance, that would clearly violate Article 8 of the Convention. The U.K. acceptance of personal data acquired under standards below the requirements of the Convention can risk circumventing a party's Article 8 obligations. Accordingly, EPIC submits that the shortcomings in U.S. surveillance authorities necessarily pollute communications intelligence data transferred to the U.K.

April 22, 2019

Respectfully submitted:

Marc Rotenberg, President
Alan J. Butler, Senior Counsel
Eleni Kyriakides, International Counsel
Electronic Privacy Information Center (EPIC)
1718 Connecticut Avenue, NW, Suite 200
Washington, DC 20009
+1 (202) 483-1140

[61] Ibid.
[62] *See* 50 U.S.C. § 1806(c—d) (providing strictly limited notification obligation); Human Rights Watch, *supra* note 12.
[63] *Zakharov*, § 234.