**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

---

## Introduction

1. The Electronic Privacy Information Center ("EPIC") welcomes the opportunity to submit these written comments pursuant to leave granted on February 26, 2016, by the President of the First Section under Rule 44 §3 of the Rules of the Court. These submissions do not address the facts or merits of the applicants' case.
2. EPIC is a public interest, non-profit research and educational organization based in Washington, D.C. [1] 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. EPIC routinely files amicus briefs in U.S. courts, pursues open government cases, defends consumer privacy, coordinates non-profit participation in international policy discussions, and advocates before legislative and judicial organizations about emerging privacy and civil liberties issues. EPIC is a leading privacy and freedom of information organization in the US with special expertise in government surveillance related legal matters.
3. The matter before the Court in *10 Human Rights Organizations and Others v. the United Kingdom* impacts the human rights to privacy, data protection and freedom of expression of people around the world, which is reflected also by the variety of the applicants' affiliations. The matter before the Court is an issue of broad international importance because it involves arrangements to transfer personal data between the United States and European countries.

*Summary of intervention.* EPIC will provide the Court with information concerning the scope and nature of surveillance conducted by the U.S. National Security Agency, which has a special relevance to this case. Specifically, EPIC will discuss (1) the National Security Agency's capacity for wide scale surveillance and the legal structures in the United States governing NSA activities, including a brief history of the surveillance activities revealed in documents released by Edward Snowden, (2) the impact of recent reform proposals in the U.S. on privacy protections for non-U.S. persons, and finally (3) current trends in U.S. and European surveillance law that are undermining privacy, data protection, and security.

[1] EPIC, *About EPIC* (2016), https://epic.org/about.

## I. The National Security Agency Collects Personal Data From Around the World and Transfer That Data Without Adequate Legal Protections

*The NSA Has Access to the Majority of Internet Traffic and a Nearly Unbounded Capacity to Monitor and Collect Private Communications*

4. One of the primary functions of the U.S. National Security Agency ("NSA") is to collect Signals Intelligence ("SIGINT") derived from "electronic signals and systems used by foreign targets, such as communications systems."[2] This includes information about "foreign powers, organizations, or persons."[3] The NSA collects communications from a variety of sources, including: (1) Internet communications flowing through "backbone" cables both inside and outside of the United States, (2) data stored by Internet service providers, (3) records stored by other telecommunications companies, and (3) intercepted satellite and radio signals.[4] The NSA's core mission is to collect as much information as possible about the activities of individuals and organizations across the globe.[5]

5. More recently, the NSA and other intelligence agencies have focused on collecting raw Internet data to monitor the communications and activities of users worldwide. According to the NSA, the nature of modern communications requires the agency to "live on the network" and gain access to all Internet signals.[6] The sheer quantity of raw Internet data collected and stored by the NSA each day is "stunning," with at least 150 sites around the globe processing billions of records per day.[7] The GCHQ has taken a similar approach, tapping more than 200 fiber optic cables by 2013 and expanding their technical abilities to process many "terabytes (thousands of gigabytes) of data at a time."[8]

6. The NSA collects such a large quantity of Internet communications that it has had to vastly expand its data-gathering apparatus. The NSA recently built a $2 billion data center in Buffdale, Utah, that was designed to house a "yottabyte – or one thousand trillion gigabytes – of data."[9] As a result, the huge volumes of Internet data collected at

---

[2] NSA, "Signals Intelligence" (2009), https://www.nsa.gov/sigint/.
[3] *Id*.
[4] Jason Stray, *FAQ: What You Need to Know About the NSA's Surveillance Programs*, ProPublica (Aug. 5, 2013), https://www.propublica.org/article/nsa-data-collection-faq; *see also* James Bamford, *The NSA is Building the Country's Biggest Spy Center (Watch What You Say)*, Wired (Mar. 15, 2012), http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/.
[5] *See generally* James Bamford, *The Puzzle Palace: Inside the National Security Agency, America's Most Secret Organization* (1st ed. 1983); James Bamford, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency* (reprt. ed. 2002); James Bamford, *The Shadow Factory: The NSA from 9/11 to the Eavesdropping on America* (2009).
[6] National Security Agency, *Transition 2001* at 31 (Dec. 2000), *available at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB24/nsa25.pdf.
[7] *See* Bruce Schneier, *More About the NSA's XKEYSCORE*, Schneier on Security (July 7, 2015), https://www.schneier.com/blog/archives/2015/07/more_about_the_.html; Micah Lee, Glenn Greenwald, & Morgan Marquis-Boire, *Behind The Curtain: A Look at the Inner Workings of NSA's XKEYSCORE*, The Intercept (July 2, 2015), https://theintercept.com/2015/07/02/look-under-hood-xkeyscore/; Glenn Greenwald, *XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet'*, The Guardian (July 31, 2013), http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.
[8] Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies, & James Ball, *GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications*, The Guardian (June 21, 2013), http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.
[9] Press Release, Utah Governor Gary R. Herbert, 2012 Energy Summit, http://blog.governor.utah.gov/2012/02/2012-energy-summit/.

sites around the world can now be stored in a centralized location – the Utah Data Center. The only technology that currently prevents "untrammeled government access to private digital data" is strong encryption.[10] But the NSA is already working to break one of the most common strong encryption standards, the "Advanced Encryption Standard," using a new supercomputer housed in the agency's Tennesee facility.[11]

7. In order to facilitate its broad surveillance activities, the NSA depends on private contractors and researchers to develop newer and more powerful tools to collect, store, process, and disseminate personal data. In addition to the traditional research and development model, a more direct market for surveillance technology has developed over the last 10 years into a $5 billion industry.[12] These technologies are showcased for U.S. Intelligence Agencies each year at conferences held by surveillance industry associations.[13] Documents obtained from a prior surveillance conference revealed that NSA and other intelligence agencies have the capability to make copies of "everything coming through [a network] switch" and transfer the personal data to other agencies.[14]

8. The NSA has also expanded surveillance efforts to obtain sensitive personal information about foreign citizens including their cell phone location records, their e-mail address books, and their pictures and videos sent via online chats.[15] The NSA also collects data from Internet providers related to network security.[16]

9. As these new surveillance tools continue to evolve and as NSA and other intelligence agencies continue to expand their collection and storage facilities, there will be few (if any) digital communications that are not potentially subject to surveillance.

---

[10] Bamford Wired Article, *supra*.
[11] *Id*.
[12] Jennifer Valentino-Devries et al., *Document Trove Exposes Surveillance Methods*, Wall St. J. (Nov. 19, 2011).
[13] *See* TeleStrategies, *ISS World Americas 2016*, http://www.issworldtraining.com/ISS_WASH/.
[14] The CEO of OnPath, a New Jersey company, is quoted as saying "[w]e're allowing a whole new level of intelligence in the networks . . . . We can take a copy of everything coming through our switch and dump it off to the FBI." *The Surveillance Catalog: OnPath Technologies – Notes*, Wall St. J. (2011), http://projects.wsj.com/surveillance-catalog/documents/267794-documents-266211-onpath-technologies-lawful/.
[15] *See* James Risen and Laura Poitras, *N.S.A. Collecting Millions of Faces from Web Images*, N.Y. Times (May 31, 2014), http://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html; Barton Gellman & Ashkan Soltani, *NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show*, Wash. Post (Dec. 4, 2013), http://www.washingtonpost.com/world/national- security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3- bc56-c6ca94801fac_story.html; Barton Gellman & Ashkan Soltani, *NSA Collects Millions of E-Mail Address Books Globally*, Wash. Post, (Oct. 14, 2013), http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9- 11e3-80c6-7e6dd8d22d8f_story.html..
[16] *See* EPIC, *EPIC v NSA: Google / NSA Relationship* (2016) https://epic.org/foia/nsa/google/default.html.

*U.S. Law Does Not Limit the NSA's Collection of Non-U.S. Persons' Data*

10. The United States government has long taken the position that no law restricts the NSA's collection of foreign communications.[17] Instead of operating according to established statutory restrictions, the NSA operates according to structures established by the President in Executive Orders, rules promulgated by the Department of Defense, and directives established by the NSA itself.[18] Many of these rules were changed after systematic abuses by the U.S. Intelligence Community were uncovered during the Church Committee investigations in 1976, but the reforms adopted by Congress were focused on preventing the NSA and other agencies within the U.S. Intelligence Community from conducting warrantless surveillance on U.S. persons.[19] No U.S. law or regulation prohibits the NSA from conducting warrantless surveillance on foreign citizens abroad.

11. Even though the President and U.S. government agencies have established regulations and procedures governing the NSA's surveillance activities, most of these documents have not been made available to the public. The primary document that outlines the NSA's surveillance authorities is Executive Order 12333, which was issued in 1981 following the Church Committee report and passage of the Foreign Intelligence Surveillance Act in 1978.[20] The Executive Order was adopted to "enhance" the ability of the U.S. Intelligence Community to acquire foreign intelligence while providing certain limited protections for United States persons.[21] More recently, President Obama has promulgated a new directive to provide certain protections for non-U.S. persons, but these new rules do not limit the collection of communications or personal data.

12. The recent debates over the scope of NSA surveillance have underscored the lack of protections granted to non-U.S. persons. The first NSA surveillance program revealed in 2013 concerned the bulk collection of telephone call detail records and other "metadata" under "Section 215."[22] Following the disclosure of the NSA metadata program, a number of organizations filed suit alleging that the bulk collection of metadata was illegal and unconstitutional.[23] But the focus of the legal challenges and subsequent reviews by oversight bodies was on the ineffectiveness of the programs and their invalidity under

---

[17] *See* Letter from the Office of Legal Counsel, U.S. Department of Justice, to Judge Colleen Kollar-Kotelly (May 17, 2002), http://www.dni.gov/files/documents/OLC%209-with%20attachment.pdf; *see also* Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 Harv. J. L & Pub. Pol'y 117, 144–47 (2015).

[18] *See* NSA, *SIGINT Frequently Asked Questions* (2009), https://www.nsa.gov/sigint/faqs.shtml#sigint6.

[19] 1 Kris & Wilson, *National Security Investigations & Prosecutions* § 2:2 History of Abuse (2d ed. 2012).

[20] *Id*. § 2:7 Increased Regulation and Oversight; *see also* Amos Toh, Faiza Patel, & Elizabeth Goitein, Brennan Center for Justice, *Overseas Surveillance in an Interconnected World* (2016), https://www.brennancenter.org/sites/default/files/publications/Overseas_Surveillance_in_an_Interconnected_World.pdf.

[21] Exec. Order No. 12,333 § 2.2, 3 C.F.R. 200 (1981)

[22] Glenn Greenwald, *NSA Collecting Phone Records Of Millions Of Verizon Customers Daily*, The Guardian (June 6, 2013).

[23] *See In re EPIC*, 134 S. Ct. 638 (2013) (seeking mandamus review of the FISC order based on the argument that the court lacked jurisdiction to require ongoing production of all telephone metadata); *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015) (finding that the FISC order requiring production of telephone metadata exceeded the authority granted under Section 215); *Klayman v. Obama*, ___ F. Supp. 3d ___ (D.D.C. 2015) (granting injunctive relief ); *Smith v. Obama*, 24 F. Supp. 3d 1005 (D. Idaho 2014).

U.S. laws that protect U.S. persons from unwarranted surveillance.[24] The second program revealed concerned the NSA's collection of private communications from U.S.-based Internet service providers through a program codenamed "PRISM."[25] A related program called "UPSTREAM" involved the collection of communications directly from Internet telecommunications cables.[26] These two programs were largely ignored by U.S. oversight bodies even though it had previously been the subject of criticisms from privacy groups, and an unsuccessful legal challenge in the U.S. Supreme Court.[27] However, the U.S. Privacy and Civil Liberties Board, in their review of the PRISM program, did acknowledge that the lack of legal protections for non-U.S. persons "raises important but difficult legal and policy questions" because "privacy is a human right" recognized under the ICCPR, despite the fact that they found that it complied with U.S. law.[28]

13. Given the lack of legal restrictions and the broad scope of NSA's surveillance activities overseas, it is clear that a significant amount of personal information and private communications of non-U.S. persons is being collected and processed without adequate protection.

*NSA Has a Long History of Conducting Surveillance in Collaboration With GCHQ*

14. The NSA has routinely entered into data transfer agreements with the GCHQ and other EU intelligence agencies. These surveillance agreements became a matter of public concern in 2000, when the European Parliment began an investigation into the activities. The investigation focused on a program known as "ECHELON," a data sharing agreement involving the UK, the USA, Canada, Australia and New Zealand ("UKUSA") for the purposes of intelligence interception.[29] While the NSA and its UKUSA intelligence partners had been exchanging intercepted communications since the beginning of their partnership in 1946, the development of ECHELON allowed the

---

[24] *See* Privacy and Civil Liberties Oversight Board, *Report on the Telephone Record Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court* 11 (Jan. 23, 2014) (finding that the program was ineffective and likely violated U.S. law), http://perma.cc/FA8U-6RFJ; Review Group on Intelligence and Communication Technologies, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies* 104 (2013) (finding that the program was not necessary)..

[25] *Id*.

[26] *See* Siobhan Gorman & Jen Valentino-Devries, *New Details Show Broader NSA Surveillance Reach*, Wall St. J. (Aug. 20, 2013), http://www.wsj.com/articles/SB10001424127887324108204579022874091732470; Craig Timburg, *NSA Slide Shows Surveillance of Undersea Cables*, Wash. Post (July 10, 2013), https://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html.

[27] *See also FISA Amendments Act of 2008: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary*, 112th Cong. 27–37 (2012) (Statement of Marc Rotenberg, Executive Dir., EPIC); *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013).

[28] Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* 8–9 (2014), https://www.pclob.gov/library/702-Report.pdf.

[29] European Parliament: Temporary Committee on the ECHELON Interception System, *Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON Interception System)*, 1 July 2001, available at: http://www.fas.org/irp/program/process/rapport_echelon_en.pdf.

UKUSA partners to pool all of their signals intelligence data automatically.[30] As a result, "agencies would be able to submit targets to one another's listening posts and, likewise, everyone would be allowed to share in the take – to dip their electronic ladles into the vast cauldron of intercepts and select what they liked."[31]

15. Since the ECHELON program was uncovered, the NSA and GCHQ have expanded their surveillance collaboration even further to collect increasingly sensitive information about Europeans. The NSA has worked with GCHQ on a program (MUSCULAR) to tap cables connecting some of the largest Internet service providers and gained access to e-mail address books, contact lists, and other private information.[32] The NSA collaborated with GCHQ on a program (OPTIC NERVE) to collect images from video chats among millions of Yahoo! users, including images of their faces and other sensitive materials.[33] The NSA collects the content and metadata of hundreds of millions of text messages under a program (DISHFIRE) where both GCHQ and NSA mine data to obtain contacts, location information, and credit card details.[34] More recently, it was revealed that GCHQ assisted the NSA in collecting sensitive personal information about cell phone users that was generated by cell phone applications such as Google Maps and Angry Birds.[35]

**16.** These covert surveillance activities are inconsistent with the U.S. and U.K. obligations under various international human rights laws and treaties.[36]

## II. Domestic Surveillance Reforms in the U.S. Do Not Provide Meaningful Privacy Protections for Non-U.S. Persons

17. There have been recent efforts to reform U.S. surveillance law in both the executive and legislative branches; however, these reforms have been limited in scope and do not limit the collection of data about non-U.S. persons overseas. Following the NSA revelations in 2013, Congress held a series of hearings and proceeded to consider a number of different reform proposals. Ultimately, these efforts resulted in the passage of the USA

---

[30] James Bamford, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency*, 394-404 (1st ed. 2002).
[31] *Id*. at 404.
[32] Barton Gellman & Ashkan Soltani, *NSA Collects Millions of E-mail Address Books Globally*, Wash. Post (Oct. 14, 2013), https://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html; Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, Wash. Post (Oct. 20, 2013), 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.
[33] Spencer Ackerman & James Ball, *Optic Nerve: Millions of Yahoo Webcam Images Intercepted by GCHQ*, The Guardian (Feb. 28, 2014, 5:31 AM), http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo.
[34] James Ball, *NSA Collects Millions of Text Messages Daily in 'Untargeted' Global Sweep*, The Guardian (Jan. 16, 2014), http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep.
[35] Julia Angwin and Je Larson, *FAQ About NSA's Interest in Angry Birds and Other Leaky Apps*, ProPublica (Jan. 28, 2014), https://www.propublica.org/article/faq-about-nsas-interest-in-angry-birds-and-other-leaky-apps; Jeff Larson, James Glanz & Andrew W. Lehren, *Spy Agencies Probe Angry Birds and Other Apps for Personal Data*, ProPublica (Jan. 27, 2014) https://www.propublica.org/article/spy-agencies-probe-angry-birds-and-other-apps-for-personal-data.
[36] ICCPR art. 17., UDGR art. 12. and Mutual Legal Assistance Treates.

FREEDOM Act in June 2015.[37] The President issued an order in January of 2014, which outlined a plan to impose new Intelligence Community rules concerning non-U.S. persons.[38] The reforms, however, have not provided adequate protection for non-U.S. persons or limited the amount of data collected abroad.

18. **USA FREEDOM Act.** Beginning in 2013, the U.S. Congress considered a number surveillance reform proposals, which focused primarily on three issues: (1) ending bulk collection of Americans' telephony metadata under Section 215 of the Patriot Act; (2) increasing transparency of surveillance activities through public reports and audits; and (3) improving oversight and transparency of the Foreign Intelligence Surveillance Court process.[39] The USA FREEDOM Act, which was subsequently passed in 2015, addressed some, but not all, of the issues raised Congress.[40] The Freedom Act included a number of significant changes to surveillance programs and oversight mechanisms, but the central component of the law was a reformulation of Section 215.[41] The law bans bulk collection under Section 215,[42] instead requiring that the government base an application for "call detail records" (CDR) on a "specific selection term."[43] In addition to the changes to Section 215 and the prohibition on bulk collection, the Freedom Act also includes provisions imposing new disclosure requirements for significant FISC opinions and orders, creating a panel of amici curiae to provide the FISC with assistance on legal and technical matters, and addressing some concerns about the targeting of United States persons under Section 702.[44]

19. **PPD-28.** While Congress was pursuing legilsative reforms to Section 215, the President issued a new directive concerning the government's use of electronic surveillance and the privacy impact of its signals intelligence programs.[45] The new Presidential Directive, PPD-28, required members of the Intelligence Community to develop and implement

---

[37] USA FREEDOM Act of 2015, Pub. L. 114-23, 129 Stat. 268.

[38] *See* Press Release, *Presidential Policy Directive–Signals Intelligence Activities* (Jan. 17, 2014), https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

[39] *See generally* Alan Butler, *Standing Up to Clapper: How to Increase Transparency and Oversight of FISA Surveillance*, 48 New Eng. L. Rev. 55, 91–100 (2013).

[40] Steve Vladeck, *The Second Circuit and the Politics of Surveillance Reform*, Just Security (May 7, 2015), https://www.justsecurity.org/22839/circuit-politics-surveillance-reform/.

[41] *See USA Freedom Act: What's In, What's Out*, Wash. Post (June 2, 2015), https://www.washingtonpost.com/graphics/politics/usa-freedom-act/; Alan Butler, *NSA Reform Moves Forward in Congress—With a Clear Prohibition on Bulk Collection But Still Missing Important Transparency and Oversight Provisions*, Privacy Rights Blog@epic.org (May 14, 2014), http://epic.org/blog/2014/05/nsa-reforms-move-forward.html.

[42] Pub. L. 114-23 § 103, 129 Stat. 268, 272 (2015). The law also prohibits bulk collection under the FISA Pen Register provision. *See* Pub. L. 114-23 § 201, 129 Stat. 268, 277 (2015).

[43] Pub. L. 114-23 § 101, 129 Stat. 268, 269–270 (2015). In order to obtain a CDR order, the government must submit the application to the FISC and show that (1) it has "reasonable grounds" to show that the CDRs related to that specific selection term are "relevant" to an investigation, and (2) it has a "reasonable articulable suspicion" that the selection term is "associated with a foreign power engaged in international terrorism." Pub. L. 114-23 § 101(a)(3), 129 Stat. 268, 270 (2015). If the FISC grants the application, then the government can order a company to provide CDRs within "two hops" of the specific selection term. *See* Jodie Liu, *So What Does the USA Freedom Act Do Anyway?*. LawFareBlog (June 3, 2015), https://www.lawfareblog.com/so-what-does-usa-freedom-act-do-anyway.

[44] *Id*.

[45] *See* Remarks on United States Signals Intelligence and Electronic Surveillance Programs, 2014 Daily Comp. Pres. Doc. 30 (Jan. 17, 2014).

certain privacy protections for their surveillance programs.[46] The PPD included six sections, the last two concerning reports and jurisdictional effects and the first four outlining policy guidance, limitations, and rules for signals intelligence.[47] But while the PPD does impose new rules limiting retention and dissemination of non-U.S. persons' information, it does not limit its collection. Most significantly, while the PPD is binding on executive branch agencies, but does not create a right of action enforceable in court.[48]

20. **The Umbrella Agreement.** The US and EU are in the midst of negotiating a so-called "Umbrella Agreement", a framework for transatlantic data transfers between US and EU law enforcement agencies.[49] The proposed goal of the Agreement is to provide data protection safeguards for personal information transferred between the EU and the US. According to an independent analysis of the Agreement, in its current form, do more harm than good for Europeans. It does not provide for adequate safeguards but violates the EU Charter of Fundamental Rights[50]. The finalization and signing of the agreement depends on adoption of the Judicial Redress Act 2015.

21. **Judicial Redress Act.** By tradition, the US Privacy Act does not provide legal rights for individuals who are not US citizens or lawful permanent residents.[51] A recent amendment called Judicial Redress Act ("JRA") may provide certain narrow claims in contingent circumstances. At present there has been no change regarding the legal rights of non-US persons under the Privacy Act. The need to extend privacy safeguards to non-U.S. persons arises from the concern that personal information transferred from the European Union to the United States lacks adequate privacy protection. The Judicial Redress Act simply does not provide for adequate safeguards.[52] Before the final vote in Congress, JRA was amended and the very limited safeguards it would have offered was weakened

---

[46] Directive on Signals Intelligence Activities, 2014 Daily Comp. Pres. Doc. 31 (Jan. 17, 2014).

[47] *See generally id*. The first section requires that all signals intelligence collection be "conducted consistent with" four principles: (1) executive branch authorization (2) purpose limitation and consideration of privacy and civil liberties impact, (3) prohibition on collecting foreign private commercial information for competitive advantage, and (4) narrow tailoring of collection activities. The second section imposes limitations on the use of signals intelligence collected in bulk, namely that such information may only be used for six listed purposes: espionage, terrorism, weapons of mass destruction, cybersecurity, threats to armed forces, and transnational crime. The third section requires an annual review of signals intelligence policies and procedures by all Intelligence Community leaders in light of the PPD-28 principles. And finally the fourth section requires that all Intelligence Community agencies develop and adopt safeguards to protect the personally information of any person (regardless of nationality) collected through the signals intelligence programs.

[48] Peter Swire, "US Surveillance Law, Safe Harbor, and Reforms Since 2013" (Dec. 17, 2015).

[49] Agreement Between The United States of America and The European Union on The Protection of Personal Information Relating to The Prevention, Investigation, Detection, and Prosecution of Criminal Offenses, http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf.

[50] Douwe Korff, *EU-US Umbrella Data Protection Agreement : Detailed Analysis*, FREE Group (October 14, 2015), http://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/.

[51] 5 U.S.C. § 552a(a)(2). *See generally, The Privacy Act 1974*, EPIC (2015), https://epic.org/privacy/1974act/.

[52] EPIC, *EPIC Recommends Changes to Judicial Redress Act* (Sept. 16, 2015), https://epic.org/2015/09/epic-recommends-changes-to-jud.html.

even more with the introduction of a national security exemption.[53] Moreover, the NSA has sought to exempt itself from all Privacy Act obligations, even for U.S. citizens.[54]

22. **Commercial data flows between the EU and the U.S.** On February 29, 2016, the European Commission and the U.S. Department of Commerce released the proposed EU-U.S. Privacy Shield. The Privacy Shield aims to replace the Safe Harbor framework for commercial data flows between the EU and the U.S., which was struck down by the Court of Justice of the European Union in October 2015. The Privacy Shield agreement is to serve as the basis for an "adequacy" decision by the European Commission that the U.S. has a satisfactory system regarding data protection, including addressing issues related to government surveillance and consumer privacy. This scheme does not adequately protect consumers' fundamental rights to privacy and data protection, as established in the EU Charter of Fundamental Rights and the 1995 Data Protection Directive, seen in the light of the European Court of Justice decision on 'Safe Harbor'[55]. The failure of the US to enact legislation on meaningful surveillance reform and to have a robust overarching data protection law that ensures the privacy of its own citizens and consumers creates a barrier to any serious consideration on adequacy.[56] EPIC believes that the Privacy Shield will fail under the legal scrutiny of European Data Protection Authorities and, eventually, the European Court of Justice.[57]

23. The U.S. has failed to adopt meaningful reforms and to make necessary changes in its domestic laws and international commitments to provide adequate (and essentially equivalent) privacy and data protection safeguards for non-U.S. persons regarding the commercial, law enforcement and national security data collections and use.

## III. Both the U.S. and EU Member States Seek to Undermine Privacy and Data Security

24. The protection for the fundamental rights to privacy and data protection as guaranteed by the European Convention on Human Rights has been weakened by many countries' (including the US and EU Member States, and the UK in particular) efforts to adopt legislations for new, more intrusive surveillance powers and attacks on constitutional checks and balances since this case was brought before the Court.

25. Furthermore, the ongoing trend in the U.S. and abroad is to weaken fundamental privacy rights. President Obama has drafted a proposed framework to increase the transfer of personal data collected NSA to other countries, reducing legal protections.[58] The Federal Bureau of Investigation is pushing again for limitations on device security and are seeking to undermine strong encryption that is essential to protect consumers from crime

---

[53] Eric Geller, *Everything You Need to Know About The Big New Data-Privacy Bill in Congress*, Daily Dot (Feb. 4, 2016), available at http://www.dailydot.com/politics/what-is-the-judicial-redress-act-europe-data-privacy-bill/.

[54] *See* EPIC, *NSA Petition* (2013), https://epic.org/NSApetition/.

[55] Judgement of 6 October 2015, Case-362/14

[56] Marc Rotenberg, Testimony before the LBE Committee of the European Parliament (March 17, 2016) http://www.europarl.europa.eu/ep-live/en/committees/video?event=20160317-1500-COMMITTEE-LIBE.

[57] EPIC, *Transatlantic Coalition of Civil Society Groups: Privacy Shield Is Not Enough, Must Return to Negotiating Table* (March 16, 2016), https://epic.org/privacy/intl/schrems/Priv-Shield-Coalition-LtrMar2016.pdf.

[58] Charlie Savage, *Obama Administration Set to Expand Sharing of Data That N.S.A. Intercepts*, N.Y. Times (Feb. 25, 2016), available at http://www.nytimes.com/2016/02/26/us/politics/obama-administration-set-to-expand-sharing-of-data-that-nsa-intercepts.html?_r=1.

and theft.[59] And the the U.S. Intelligence Community has refused to follow treaty requirements on human rights.[60] The UK is leading efforts in Europe to broaden surveillance authorities and weaken encryption protections.[61]

26. The right to privacy and security are not conflicting interests. Governments must move past the argument that there is a trade-off between privacy and security. In reality, privacy, encryption, and national security are mutually supportive goals. Privacy and data protection are essential for the effective excersise of individual rights to freely form and express opinions. Mass surveillance programs have a chilling effect on journalists, human rights defenders, and whistleblowers, including the applicants in this case.

**Conclusion**

27. EPIC submits that facts outlined above support the conclusion that NSA-UK data transfers violate the Convention for at least three reasons.

28. First, the evolving technological capabilities of the NSA and other intelligence agencies create an almost unlimited ability to access, store and use personal information and private communications globally. The lack of legal restrictions on the United States' surveillance activities overseas mean that a significant amount of personal information of non-U.S. persons is being collected and processed without adequate protection.

29. Second, recent reforms have not provided adequate safeguards for non-U.S. persons against these surveillance activities.

30. Third, both the United States and EU Member States are moving toward laws and measures that further undermine privacy and security.

March 18, 2016

Respectfully submitted:

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

[59] Corrected Brief of Electronic Privacy Information Center (EPIC) and Eight Consumer Privacy Organizations, In re Apple, No. 16-cm-00010 (C.D. Cal. March 3, 2016), available at https://epic.org/amicus/crypto/apple/EPIC-Corrected-Amicus-Brief.pdf.

[60] Access Now, *Intelligence Community Refuses to Follow Treaty Requirements on Human Rights* (March 14, 2016), https://www.accessnow.org/intelligence-community-refuses-follow-treaty-requirements-human-rights/.

[61] *See* Scarlet Kim, *The Snooper's Charter Is Flying Through Parliament. Don't Think It's Irrelevant To You*, The Guardian (March 14, 2016) http://www.theguardian.com/commentisfree/2016/mar/14/snoopers-charter-apple-fbi-bill-hacking-gagging; Privacy International, *Investigatory Powers Bill Published: Minimal Changes Are Not Even Cosmetic* (March 1, 2016) https://www.privacyinternational.org/node/771.