epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

Comments of the
ELECTRONIC PRIVACY INFORMATION CENTER

OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS
Call for inputs to a report on "the right to privacy in the digital age"

April 6, 2018

The Electronic Privacy Information Center ("EPIC") submits the following comments to the Office of the High Commissioner for Human Rights ("OHCHR"), pursuant to the on "Call for inputs to a report on 'the right to privacy in the digital age.'"[1]

EPIC is a public interest research center in Washington, D.C. 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.[2] EPIC frequently testifies before Congress,[3] participates in the administrative agency rulemaking process, [4] and litigates landmark privacy cases in the U.S.[5]

EPIC has also played a pivotal role in the international development of privacy law and policy. EPIC established the Public Voice project in 1996 to enable civil society participation in decisions concerning the future of the Internet.[6] EPIC seeks widespread adoption of the Madrid Privacy Declaration, a document drafted in 2009 in tandem with the 31st International Conference of Data Protection and Privacy Commissioners.[7] The Declaration "reaffirms international instruments for privacy protection, identifies new challenges, and call[s] for concrete actions" and has been signed by hundreds of organizations and experts.[8] EPIC also publishes *Privacy and Human Rights*, a

---

[1] UN Office of the High Comm'r, *Call for inputs to a report on "the right to privacy in the digital age,"* Ohchr.org, http://www.ohchr.org/EN/Issues/DigitalAge/Pages/ReportPrivacy.aspx.
[2] *See*, About EPIC, *EPIC, https://epic.org/epic/about.html.*
[3] https://epic.org/testimony/congress/
[4] https://epic.org/apa/comments/
[5] https://epic.org/privacy/litigation/#cases
[6] *See*, About the Public Voice, *The Public Voice*, http://thepublicvoice.org/about-us/.
[7] The Madrid Privacy Declaration (2009), http://www.thepublicvoice.org/Madrid-declaration/.
[8] *Id*.

comprehensive review of privacy laws and developments around the world, and the *Privacy Law Sourcebook*, which includes many of the significant privacy frameworks..[9]

We appreciate the opportunity to provide input into the OHCHR's upcoming report on the right to privacy around the world. With the "Call for inputs to a report on 'the right to privacy in the digital age'" OHCHR seeks submissions on recent developments in national or regional legislation, surveillance and communications interception, and frameworks for collection, processing, retention or use of personal data by Governments and business enterprises.[10] Based on this request, EPIC seeks to update the Office of the High Commissioner on the latest developments concerning U.S. surveillance and law enforcement access to personal data, in part I, U.S. consumer privacy protection, in part II, and the work of the Special Rapporteur on Privacy, in part III.

I. Surveillance & Law Enforcement

A. CLOUD Act Establishes Unilateral Law Enforcement Access to Foreign Data

As a result of a global digital communications landscape, law enforcement increasingly seeks communications data stored outside national borders in domestic criminal investigations. However, foreign access can conflict with national data protection regimes and international human rights instruments. [11] As a result, the terms of tans-border access should be established via international consensus.[12] However, the Clarifying Lawful Overseas Use of Data (CLOUD) Act, signed into law on March 23, 2018, provides trans-border access to communications data in criminal law enforcement investigations. The Act's history begins with a privacy dispute between Microsoft and the U.S. government.[13] In *United States v. Microsoft*, the U.S. Supreme Court was considering whether law enforcement agents in the United States can compel a US Internet company to turn over personal data stored in a foreign jurisdiction.[14] With the passage of the CLOUD Act, the Department of Justice moved to dismiss the case. [15]

---

[9] EPIC, *Privacy and Human Rights: An International Survey of Privacy Laws and Developments* (ed. M. Rotenberg EPIC 2006) and EPIC, *The Privacy Law Sourcebook 2016: United States Law, International Law, and Recent Developments* (ed. M. Rotenberg EPIC 2016), available at https://epic.org/bookstore/.

[10] UN Office of the High Comm'r, *supra* note 1.

[11] Brief for EPIC and Thirty-Seven Technical Experts and Legal Scholars as Amici Curiae in Support of Respondent, *United States v. Microsoft*, No. 17-2 (Jan. 18, 2018), https://epic.org/amicus/ecpa/microsoft/US-v-Microsoft-amicus-EPIC.pdf.

[12] *Id.*

[13] Consolidated Appropriations Act, 2018, H.R. 1625, Div. V, 115th Cong., 2d Sess. (2018) (including the CLOUD Act) [hereinafter CLOUD Act].

[14] EPIC, *United States v. Microsoft*, Epic.org, https://epic.org/amicus/ecpa/microsoft.

There are two key elements of the CLOUD Act - the provisions for U.S. access to foreign stored data, and the provisions to create executive agreements for foreign access to U.S. stored data. First, the Act amends U.S. law to allow U.S. law enforcement to unilaterally access to data stored outside the U.S. over widespread criticism of many in the international community.[16] Where the U.S. orders a company to produce communications data, the Act allows a provider to challenge the order where complying would risk violating foreign law. Under the CLOUD Act, defense of individual rights depends entirely on the objection by a provider. There is no direct mechanism for individuals to challenge an order under the CLOUD Act. A court will consider the order, including using a "comity" analysis to assess foreign interests at stake. A U.S. court may still require production of that communications data over that objection, even where the laws of another nation would be violated.

The Act would also permit federal officials to enter into executive agreements granting foreign access to data stored.[17] Federal officials must first decide a foreign government gives sufficient protection to privacy and civil liberties, and the foreign government must agree to abide by certain other limitations, including minimizing any U.S. person data collected. The initial agreement need only be certified by executive branch officials to take effect. Can Congress can object to the agreement, but need not formally approve the agreement. The agreement is unreviewable in court.

After an executive agreement is in place, U.S. federal officials and courts will not review any incoming foreign request for communications data stored in the U.S. - whether to ensure that request complies with the requirements of the executive agreement or otherwise. The communications company, alone, will have an opportunity to review and object to a foreign request it receives. However, there are no formal procedures under the CLOUD Act for a provider to object to a request made under an executive agreement.

Because the executive agreement would permit data to be accessed by foreign nations based on each nation's unique domestic procedures, data is accessible using domestic provisions that may also fall below human rights standards. For instance, the CLOUD Act does not require notice to be provided to the target of a request for communications data stored in the U.S.

Similarly, foreign requests routed through the U.S. via diplomatic request previously benefitted from certain U.S. legal protections for communications data, including a requirement to demonstrate "probable cause" to access communications content. The law's provisions concerning executive agreements would erode this incidental, yet impactful, data protection benefits.

Finally, the CLOUD Act's authorization of executive agreements also undermines communications privacy protections for U.S. persons. Data collected by foreign governments under may be transferred to the U.S. government and among other governments. In order for a foreign

---

[15] Motion to Vacate the Judgment of the Court of Appeals and Remand the Case with Directions to Dismiss as Moot, United States v. Microsoft, No. 17-2 (Mar. 2018).
[16] CLOUD Act § 3.
[17] CLOUD Act § 5.

country to transfer U.S. persons' communications content to U.S. authorities, the communications must merely be determined to "relate[] to significant harm" or a "threat thereof" and non-content information may be transferred without limitation. Under these provisions, the U.S. government could access U.S. persons' communications below existing U.S. legal standards. The law also permits real-time interception of communications by foreign governments on U.S. soil for the first time, and does so without requiring other countries meet the "supper warrant" bar required to wiretap under U.S. law.

In an *amicus brief* submitted in *United States v. Microsoft*, EPIC urged the Supreme Court to respect international privacy standards, citing key cases from the European Court of Human Rights and the European Court of Justice.[18] EPIC warned that "a ruling for the government would also invite other countries to disregard sovereign authority."[19]

B. Section 702 Reauthorized without Privacy Safeguards

Congress has renewed "Section 702" of the Foreign Intelligence Surveillance Act without new privacy safeguards for U.S. persons or non-U.S. persons.[20] Section 702 of Foreign Intelligence Surveillance Act authorizes broad-based surveillance of non-U.S. persons located outside of the U.S. with the compelled assistance of electronic communications service providers.[21] Section 702 contains no requirement to demonstrate probable cause or that a target is engaged in criminal activity, nor does it require judicial review of individual surveillance orders. The FISA Amendments Reauthorization Act, passed in January 2018, extends 702 for six years.[22]

Three elements of the reauthorization bill raise special data protection and privacy concerns: the Act's failure to extend any privacy protections to non-U.S. persons, express authorization for "about" collection to be restarted, and its failure to limit "backdoor searches" of U.S. person communications.

Failure to Extend Privacy Protection to Non-U.S. Person

The FISA Amendments Reauthorization Act did not extend privacy protection to non-U.S. persons. U.S. foreign intelligence surveillance practices have been contested around globe for the failure to respect the fundamental privacy rights of non-U.S. persons. The debate culminated in the landmark 2015 European Court of Justice *Schrems* decision overturning the Safe Harbor agreement

[18] Brief for EPIC and Thirty-Seven Technical Experts and Legal Scholars as Amici Curiae in Support of Respondent, United States v. Microsoft, No. 17-2 (Jan. 18, 2018), https://epic.org/amicus/ecpa/microsoft/US-v-Microsoft-amicus-EPIC.pdf.
[19] *Id.*
[20] EPIC, *Foreign Intelligence Surveillance Act (FISA)*, Epic.org https://epic.org/privacy/surveillance/fisa/.
[21] 50 U.S.C. §§ 1881a et seq.
[22] The FISA Amendment Reauthorization Act of 2018, Public Law No: 115-118, 132 Stat. 3 (2018).

– a pact for the transfer of consumer data between the EU and U.S.[23] The replacement agreement, the Privacy Shield, is under review by European institutions.[24] Without a revision of U.S. surveillance practices, it remains vulnerable to the same criticisms lodged by the CJEU.[25] Nonetheless, the extension of any privacy protections to non-U.S. persons was never meaningfully considered during the legislative debate over 702's reauthorization.

Authorization to Restart "About" Collection

The FISA Amendments Reauthorization Act expressly authorized the restarting of "about" collection. This practice involves surveillance of communications "in which the selector of a targeted person (such as that person's email address) is contained within the communication but the targeted person is not necessarily a participant in the communication."[26] Under "about" collection, the government access to private communications is broader than other means of collection because it necessarily involves scanning the content of all messages over a particular network in order to find selected terms within the body of a communication.[27] The NSA ended the program in 2017 because it was unable to comply with privacy strictures put in place by the FISC.[28] However, the Act permits the government to restart this controversial "about" collection program after providing thirty-day's notice to Congress.[29]

Failure to Limit "Backdoor Searches" for Information on Americans

The FISA Amendments Reauthorization Act also failed to limit "backdoor searches" for information on Americans, a key aspect of domestic debate over 702.

Federal agencies can search communications collected under Section 702 for information about Americans (a "backdoor search"), even though Americans *cannot not lawfully be targeted* at the front end.[30] Government published statistics confirms agencies frequently search 702 data for information about U.S. persons. In 2016, there were over 5,000 government queries using search

---

[23] Judgment 6 October 2015, *Schrems v. Irish Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650.
[24] *See, e.g.*, Article 29 Working Party, EU – U.S. Privacy Shield – First annual Joint Review (2017), http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782.
[25] *Id.*
[26] Privacy and Civil Liberties Oversight Bd., *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* 7 (2014) [hereinafter PCLOB 702 Report].
[27] *Id*.
[28] Statement, NSA Stops Certain Section 702 "Upstream" Activities (Apr. 28, 2017), https://www.nsa.gov/news-features/press-room/statements/2017-04-28-702-statement.shtml.
[29] FISA Amendment Reauthorization Act § 2.
[30] Priv FISA Amendment Reauthorization Act acy and Civil Liberties Oversight Bd*., Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* 59 (2014), https://www.pclob.gov/library/702-report.pdf.

terms concerning *known* U.S. persons to retrieve the unminimized contents of communications.[31] There were 30,355 queries concerning a known U.S. person of metadata obtained under 702.[32] Importantly, even these statistics are underinclusive – they exclude FBI queries.[33]

Despite heated debate over the Intelligence community practice and *the illusion of a statutory fix*, these "backdoor searches" were reauthorized by the FISA Amendments Reauthorization Act.[34] The Act does require the FBI to obtain a court order in strictly limited circumstances: where the agency wants to search 702 data for information about U.S. persons in a criminal law enforcement investigations.[35] However, the FBI need only obtain an order if it is in a *late stage* criminal investigation, if it wants to view the contents of a communication, and, even then, subject to exception.[36] The FBI is also still able to conduct "backdoor searches" at earlier phases of an investigation with little factual basis, or for broadly defined purposes like "foreign intelligence."[37] Other federal agencies' practices are also untouched by the Act.[38] In short, the FISA Amendments Reauthorization Act leaves a "backdoor search" loophole intact.

C. Missing Oversight: Privacy and Civil Liberties Oversight Board Vacancies & Delayed Reports

Privacy and Civil Liberties Oversight Board (PCLOB) has been unable to act due to long-term vacancies on the board, and has still not published multiple long-promised oversight reports. The PCLOB, established by the recommendation of the 9/11 Commission, provides oversight and advice over U.S. intelligence activities.[39] However, it currently has no Chair and has had only one out of its four board members since January 2017.[40] Without a quorum, the PCLOB cannot initiate new activities nor provide advice in an official capacity.[41]

The PCLOB's report on 702 in the aftermath represented pivotal moment for U.S. intelligence transparency and reform.[42] However, after four years that report is now outdated since practices and the law have both changed. The PCLOB has long promised to release reports on Executive Order 12333, which governs most of U.S. foreign surveillance, and Presidential Policy

---

[31] Office of the Dir. Of Nat'l Intelligence, *Statistical Transparency Report Regarding the Use of National Security Authorities for Calendar Year 2016* (2017).
[32] *Id.*
[33] *Id.*
[34] FISA Amendment Reauthorization Act § 2.
[35] Office of the Dir. Of Nat'l Intelligence, *supra* note 41.
[36] FISA Amendment Reauthorization Act § 2.
[37] *See, e.g.*, Letter from Coalition of 58 Organizations to Chairman Bob Goodlatte, House Judiciary Comm., and Ranking Member Conyers, House Judiciary Comm. (Oct. 3, 2017), https://epic.org/privacy/surveillance/fisa/Section702Backdoor-CoalitionLetter.pdf.
[38] *Id.*
[39] *History and Mission*, PCLOB.gov, https://www.pclob.gov/about/.
[40] *Id.* at 8.
[41] *Id.* at 8.
[42] *See* PCLOB 702 Report, *supra* note 36.

Directive 28, which extends certain protections to non-U.S. persons.[43] The report on EO 12333 is in a near final stage, and the report on PPD-28 is complete but still subject to presidential privilege.[44]

President Trump recently nominated three new Privacy and Civil Liberties Oversight Board Members, whose confirmation would provide a quorum. Adam Klein, a senior fellow at national security and defense think tank Center for New American Security, was nominated in Summer 2017 and has had a hearing before the Senate, but his nomination has yet to be put to Senate vote.[45] Klein has expressed the view that the privacy intrusion of certain Section 702 practices is limited.[46] In advance of his nomination hearing, EPIC urged the Senate to oppose the nomination. EPIC said that the nominee "does not appreciate the full extent of the privacy interests at stake in many of the most significant debates about the scope of government surveillance authority."[47] More recently, Ed Felten and Jane Nitze were nominated in March 2018.[48] Ed Felten is a member of the EPIC Advisory Board, is a professor of computer science and public affairs at Princeton, and was formerly the Deputy U.S. Chief Technology Officer for the White House. Jane Nitze was formerly an attorney with the Justice Department Office of Legal Counsel.

Senate approval of these three nominees would permit a quorum. However, with three new members at the organization, the PCLOB's future activities and direction are indeterminate.

II. Consumer Privacy Protection

A. Despite Record Data Breaches, U.S Still Lacks Comprehensive Privacy Legislation

Despite a consistent rise in record breaking data breaches, Congress has failed to advance any legislative proposal to increase consumer privacy. The U.S. continues to operate without comprehensive privacy legislation, relying instead on a patchwork of sectoral laws.[49]

---

[43] Privacy and Civil Liberties Oversight Bd., *Semi-Annual Report: October 2015-March 2016* (2016), https://www.pclob.gov/library/Semi_Annual_Report_August_2016.pdf.
[44] Article 29 Working party, *supra* note 34, at 3.
[45] Hearing on the Nomination of Adam Klein, 115th Cong. (2018), https://www.judiciary.senate.gov/meetings/01/24/2018/nominations.
[46] Adam Klein, *Connect the Dots to Stop Terror Plots*, Wall Street Journal (July 26, 2017), https://www.wsj.com/articles/connect-the-dots-to-stop-terror-plots-1501106621.
[47] Letter from EPIC to Chick Grassley, Chairman of the Senate Comm. on the Judiciary, and Richard Blumenthal, Ranking Member (Jan. 23, 2018), https://epic.org/EPIC-SJC-PCLOB-Jan2018.pdf.
[48] White House, *President Donald J. Trump Announces Key Additions to his Administration*, Whitehouse.gov (Mar. 13, 2018), https://www.whitehouse.gov/presidential-actions/president-donald-j-trump-announces-key-additions-administration-33/.
[49] *Examining the Current Data Security and Breach Notification Regulatory Regime: Hearing before the H. Comm. on Banking, Housing, and Urban Affairs*, 115th Con. (2018) (written testimony of Marc Rotenberg, EPIC President).

2017 marked the highest number of data breaches yet in the U.S., representing a grave lack of data security by U.S. companies.[50] The number of data breaches nearly doubled from 2016 to 2017.[51] There were a total of 159,700 cybersecurity incidents in 2017.[52] In one of the worst data breaches in U.S. history, the 2017 Equifax data breach exposed the sensitive personal information of over 145 million Americans.[53] Identity fraud increased by 16 percent in 2016, with a total of $16 billion stolen from 15.4 million U.S. consumers.[54]

While there are divergent state laws mandating breach notification, there is no uniform federal standard.[55] As a result, following the Equifax breach, legislation was introduced in Congress to begin to address U.S. data security and privacy shortcomings. For instance, the Data Breach Prevention and Compensation Act would establish an office of cybersecurity within the FTC to give it direct supervisory authority over the credit reporting industry and impose mandatory penalties for breaches involving consumer data at credit reporting agencies.[56] Other proposals would expand the Federal Trade Commission's enforcement authority over credit reporting agencies,[57] and prohibit entities from enforcing mandatory arbitrary clauses—which prohibit consumers from filing lawsuits—in data breach cases.[58]

Nonetheless, there has been no meaningful legislative action to improve U.S. consumer privacy with a uniform data breach notification requirement, much less to advance comprehensive privacy legislation. Yet, according to the Pew Research Center, 91% of U.S. consumers say that they have lost control over how personal information is collected and used by companies.[59] The same study reported that 64% of Americans supported greater regulation over how advertisers handle their personal data.[60]

---

[50] *See, e.g.*, Online Trust Alliance, Cyber Incident & Breach Trends Report (2018), https://www.otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf.
[51] *Id*.
[52] *Id*.
[53] EPIC, *143 Million US Consumers Suffer Massive Data Breach, Equifax at Fault*, Epic.org (Sept. 8, 2017), https://epic.org/2017/09/143-million-us-consumers-suffe.html.
[54] Javelin Strategy & Research, *Identity Fraud Hits Record High With 15.4 Million U.S. Victims in 2016, Up 16 Percent According to new Javelin Strategy & Research Study*, Press Release, (Feb. 1, 2017), https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16- percent-according-new.
[55] EPIC, *State Data Breach Notification Policy* (2017), https://epic.org/state-policy/data-breach/.
[56] S. 2289, 115th Cong. (2018).
[57] H.R. 5166, 155th Cong. (2018).
[58] H.R. 5165, 155th Cong. (2018).
[59] George Gao, Mary Madden, *Privacy and Cybersecurity: Key Findings From Pew Research*, Pew Research Center, (Jan. 16, 2015), http://www.pewresearch.org/fact-tank/2015/01/16/privacy/.
[60] *Id*.

EPIC testified before Congress following the Equifax breach, urging legislation to give consumers greater control of their personal data held by third parties, mandate data breach notification, and more.[61] EPIC has also consistently called for comprehensive privacy legislation and the creation of a federal data protection agency.[62]

B. FTC Fails to Protect U.S. Consumers: Cambridge Analytica Data Disclosure

While American consumers face unprecedented risks from data breaches, identity theft, ubiquitous data gathering and consumer profiling, the Federal Trade Commission (FTC) is failing to respond to the data protection crisis in the United States. The FTC regularly refuses to enforce its legal judgments against companies.[63] The most recent effect of this failure is the unlawful disclosure of 50 million Facebook user records to controversial data mining firm Cambridge Analytica.[64]

The effectiveness of the FTC depends primarily upon the agency's willingness to enforce the legal judgments it obtains against companies for deceptive or unfair corporate practices.[65] However, when the FTC does reach a consent agreement with a privacy-violating company, the Commission routinely fails to enforce it.[66] American consumers do not have a private right of action to obtain redress from unfair and deceptive trade practices, and thus the FTC's failure to enforce its own settlements has left consumers with little recourse. The cost of the FTC's failure to act are clear from the recent alleged disclosure by Facebook of 50 million personal records to Cambridge Analytica, a controversial data mining firm.

On March 18, 2018, investigative reporting revealed Facebook disclosed the personal data of 50 million users without their consent to Cambridge Analytica, the controversial British data mining firm that sought to influence the 2016 presidential election.[67]

---

[61] *Consumer Data Security and the Credit Bureaus: Hearing before the S. Comm. on Banking, Housing, and Urban Affairs*, 115th Con. (2018) (written testimony of Marc Rotenberg, EPIC President).

[62] *Examining the Current Data Security and Breach Notification Regulatory Regime: Hearing before the H. Comm. on Banking, Housing, and Urban Affairs*, *supra* note 59.

[63] Letter to Acting FTC Chair Maureen Ohlhausen, "FTC 2017: 10 Steps for Protecting Consumers, Promoting Competition and Innovation" (Feb. 15, 2017) ("*1. The FTC Must Enforce Existing Consent Orders")*, https://epic.org/privacy/internet/ftc/EPIC-et-al-ltr-FTC-02-15-2017.pdf.

[64] Letter from EPIC, et. al, to FTC Acting Chairman & Commissioner (Mar. 20, 2-018), https://epic.org/privacy/facebook/EPIC-et-al-ltr-FTC-Cambridge-FB-03-20-18.pdf.

[65] 15 U.S.C. Sec. 45(a)(1).

[66] *See EPIC v. FTC*, No. 12-206 (D.C. Cir. Feb. 8, 2012).

[67]Matthew Rosenberg, Nicholas Confessore, & Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. Times (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news.

The unlawful disclosure of user records to the data mining firm likely violated a 2011 FTC Consent Order against Facebook.[68] In 2009, EPIC and a coalition of US consumer privacy organizations filed an extensive complaint with the FTC following Facebook's repeated changes to the privacy settings of Facebook users that allowed the company to transfer user data without the knowledge or consent of the user.[69] In 2011, the FTC agreed with EPIC and the coalition of organizations and established a far-reaching settlement with the company that prevented such disclosures, prohibited deceptive statements, and required annual reporting.[70] Facebook's transfer of personal data to Cambridge Analytica were likely prohibited by this 2011 Facebook Order.

After the disclosure to Cambridge Analytica was revealed, EPIC and consumer privacy organizations wrote the Commissioners, calling on the FTC to "immediately undertake an investigation and issue a public report as to whether Facebook complied with the 2011 Order."[71] The FTC has confirmed it has an open investigation into Facebook.[72] Forty-one state attorneys general have also launched an investigation into Facebook's privacy practices.[73]

In closing, it is worth noting that the FTC, the primary privacy enforcement authority in the U.S., has also suffered from a long-term failure to fill Federal Trade Commission's leadership; without full membership, there has been little support for improving shortcomings in enforcement that contributed to the Cambridge-Analytica data disclosure. In 2017, the FTC's leadership was reduced to two out of five Commissioners.[74] The FTC has been without full membership or an appointed chairman for over a year. President Trump has recently nominated four new

---

[68] Marc Rotenberg, *How the FTC Could Have Prevented the Facebook Mess*, Techonomy (Mar. 22, 2018), https://techonomy.com/2018/03/how-the-ftc-could-have-avoided-the-facebook-mess/; Letter to Acting FTC Chair Maureen Ohlhausen, "FTC 2017: 10 Steps for Protecting Consumers, Promoting Competition and Innovation" (Feb. 15, 2017) ("*1. The FTC Must Enforce Existing Consent Orders")*, https://epic.org/privacy/internet/ftc/EPIC-et-al-ltr-FTC-02-15-2017.pdf.

[69] EPIC, et al, In the Matter of Facebook, Inc. (Complaint, Request for Investigation, Injunction, and Other Relief) (Dec. 17, 2009), https://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf.

[70] Press Release, Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises (Nov. 29, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

[71] Letter from EPIC, et. al, to FTC Acting Chairman & Commissioner (Mar. 20, 2-018), https://epic.org/privacy/facebook/EPIC-et-al-ltr-FTC-Cambridge-FB-03-20-18.pdf.

[72] Press release, Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practices (Mar. 26, 2018), https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection.

[73] Press release, Attorney General Shapiro Leads Bipartisan Coalition of State AGs in Demanding Answers from Facebook Attorney General Shapiro Leads Bipartisan Coalition of State AGs in Demanding Answers from Facebook (Mar. 26, 2018), https://www.attorneygeneral.gov/taking-action/press-releases/attorney-general-shapiro-leads-bipartisan-coalition-of-state-ags-in-demanding-answers-from-facebook/.

[74] John Hendel, Li Ahou, & Ashley Gold, *White House nominates 4 to FTC*, Politico (Jan. 25, 2018), https://www.politico.com/story/2018/01/25/trump-federal-trade-commission-seats-369456.

commissioners, while acting chairwoman Meureen Ohlhausen is poised to leave.[75] Four newly nominated FTC commissioners have been recently approved preliminarily by Senate committee, and now must be confirmed by full Senate vote.[76] An additional nominee is needed to fully staff the Commission.

III. Work of the Special Rapporteur on the Right to Privacy

We would also like to call attention to ongoing concerns about the work of the Special Rapporteur on the Right to Privacy. In 2015, the United Nations (UN) established a Special Rapporteur on the Right to Privacy (SRP) with a broad mandate to "protect" and "promote" the right to privacy set out in Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR).[77] The mandate set out the expectation that the Special Rapporteur would gather relevant information, make recommendations, raise awareness, report violations, identify emerging issues and report annually on his work. We believe the Special Rapporteur must align his activities with the mandate set out by the UN.

For instance, requirement (a) of the SRP's mandate concerns "gather[ing] relevant information" on the state of the right to privacy, and requirement (g) of the SRP's mandate concern calling attention to "alleged violations… of the right to privacy" or "situations of particularly serious concern." One of the primary mechanisms for Special Rapporteurs to defending a human right is via country visits. Approaching the end of the three-year mandate, the SRP has conducted two country visits to two western nations: the United States and France.[78] He has issued no formal reports from these visits, reports which are often among the most valuable tools to highlight specific situations of concern. EPIC would like to use the opportunity of the OHCHR's call for input to publicly urge the Special Rapporteur to call attention to the privacy practices of countries around the world, to prioritize finalizing a date for official country visits which have been requested, and to issue country reports on his completed visits promptly.

The SRP also continues to focus a significant portion of his work on what he has designated developing a "better understanding" of the right to privacy.[79] He asserts the "existence and usefulness of" Article 12 of the UDHR and Article 17 of the ICCPR are "seriously handicapped by

---

[75] *Id.*
[76] Harper Neidig, *Senate panel approves Trump's FTC nominees*, Hill (Feb. 28, 2018), http://thehill.com/policy/technology/375991-senate-commerce-approves-trumps-ftc-nominees.
[77] Human Rights Council Res. 28/16, U.N. Doc. A/HRS/RES/28/16 (Apr. 1, 2015).
[78] Press release, US could do more on privacy rights, UN rapporteur concludes after official visit (June 27, 2017), http://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=21806&LangID=E; Press release, France's leading role in the protection of privacy, despite remaining concerns, says UN privacy expert (Nov. 17, 2017), http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=22413&LangID=E.

the lack of a universally agreed and accepted definition of privacy."[80] EPIC believes this pursuit runs contrary to the purpose of the mandate, particularly since a key responsibility of a UN Special Rapporteur is the vigorous promotion and protection of the right. International law and legal precedents have already defined a fundamental human right to privacy. Cornerstones of the modern right to privacy, set out in Article 12 of the UDHR and Article 17 of the ICCPR, must be preserved.

We described many of these and other concerns in a detailed review last year for the *European Data Protection Law Review*.[81] It remains our view that it is vitally important for the Rapporteur to pursue the mandate set out in the UN Resolution and specifically to seek to promote Article 12 of the UDHR and Article 17 of the ICCPR.

IV. Conclusion

EPIC welcomes the continued attention of the United Nations High Commissioner for Human Rights to the fundamental right to privacy. We look forward to the OHCHR's final report on "the right to privacy in the digital age."

Sincerely,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President

/s/ Eleni Kyriakides
Eleni Kyriakides
EPIC International Counsel

[80] Special Rapporteur on the right to privacy, Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, ¶¶ 21, 25, U.N. Doc. A/HRC/31/64 (Mar. 8, 2016).
[81] Marc Rotenberg, *Urgent Man- date, Unhurried Response: An Evaluation of the UN Special Rapporteur on the Right to Privacy*, 3 Eur. Data Protection L. Rev. 47 (2017).