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

Submission of the

ELECTRONIC PRIVACY INFORMATION CENTER

to the

U.N. HUMAN RIGHTS COMMITTEE

"List of Issues Prior to Reporting" by the United States

January 10, 2019

In 2019, the United States will undergo a periodic review of adherence to the International Convention on Civil and Political Rights (ICCPR) by the U.N. Human Rights Committee. As the first step, the Committee will adopt a "list of issues prior to reporting" during the HRC's 125th session in March 2019, a list that forms the basis of the U.S. report to the Committee.[1] The Electronic Privacy Information Center (EPIC) writes in response to the Committee request for NGO submission of issues to the "list of issues prior to reporting."[2] EPIC urges the Committee to question the U.S. about the failure to protect individuals against violations of the right to privacy (Article 17) by non-state actors. Today, pervasive private sector tracking of movements, habits, and private communications has been met with minimal intervention by the U.S. government on behalf of individuals.[3] The failure to safeguard personal data stored in private record-keeping systems has also exposed U.S. residents to cyber attack by foreign states and foreign non-state actors.[4]

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,

---

[1] NGO Information Note, Human Rights Committee, 125th Session (4 to 29 March 2019), https://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fINF%2f125%2f27858&Lang=en.

[2] *Id.*

[3] *See, e.g.*, Marc Rotenberg, *Opinion: America Needs a Privacy Law*, N.Y. Times (Dec. 25, 2018) https://www.nytimes.com/2018/12/25/opinion/letters/data-privacy-united-states.html. apps.html?module=inline.

[4] Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say*, Wash. Post (Jul. 9, 2015), https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearancesystem-affected-21-5-million-people-federal-authorities-say/; Press release, Equifax Announces Cybersecurity Incident Involving Consumer Information (Sept. 7, 2017), https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628; Tim Starks, *U.S. indicts North Korean national for Sony hack, massive cyberattacks*, Politico (Sept. 6, 2018), https://www.politico.com/story/2018/09/06/justice-department-north-korea-sony-hack-771212.

freedom of expression, and democratic values in the information age.[5] EPIC frequently testifies before the U.S. Congress,[6] participates in the U.S. administrative agency rulemaking process,[7] and litigates landmark privacy cases.[8] EPIC has 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.[9] EPIC also publishes *Privacy and Human Rights*, a comprehensive review of privacy laws and developments around the world, and the *Privacy Law Sourcebook*, which includes many of the significant privacy frameworks.[10]

I. Proposed Issue: Protection of the Fundamental Right to Privacy with Respect to Private Sector Data Collection, Storage, and Use

EPIC urges Human Rights Committee to question the United States about the failure to protect the right to privacy (Article 17) with respect to private sector data collection and use. State parties to the ICCPR have a duty to protect individuals against human rights violations by non-state actors (Article 2). Despite record-breaking data breaches, identity theft, and extensive corporate surveillance, the U.S still lacks both comprehensive privacy legislation and a data protection authority. And, the agency with the most significant authority over privacy, the FTC, routinely fails to enforce its legal orders.

In first half of 2018, breaches increased in severity rising to a total of 3.3 million breached records.[11] In fact, "the amounts of records breached every day, hour, minute and second… almost doubled between 2017 and 2018."[12] Identity fraud has "hit an all time high" in the U.S., in 2017 affecting 16.7 million U.S. consumers in 2018 amounting to $16.8 billion stolen.[13] On a social and democratic level, the effects are also significant. Detailed tracking on mobile device apps

[5] *See*, EPIC, *About EPIC,* EPIC.org*, https://epic.org/epic/about.html.*
[6] EPIC, *EPIC Congressional Testimony and Statements,* EPIC.org*,* https://epic.org/testimony/congress/
[7] EPIC, *EPIC Administrative Procedure Act (APA) Comments,* EPIC.org*,* https://epic.org/apa/comments/
[8] EPIC, *Litigation Docket,* EPIC.org*,* https://epic.org/apa/comments/
https://epic.org/privacy/litigation/#cases
[9] *See*, *About the Public Voice*, The Public Voice, http://thepublicvoice.org/about-us/.
[10] EPIC, *Privacy and Human Rights: An International Survey of Privacy Laws and Developments* (ed. M. Rotenberg EPIC 2006) and EPIC, *The Privacy Law Sourcebook 2018: United States Law, International Law, and Recent Developments* (ed. M. Rotenberg EPIC 2018), available at: https://epic.org/bookstore/.
[11] Breach Level Index, 2018 First Half Report (2018), https://breachlevelindex.com/.
[12] *Id.*
[13]Press Release, Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study (Feb. 6, 2018), https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity.

consistently logs sensitive like location - the route to and from work, a trip to the medical center, or his or her church.[14] And unanticipated data transfers can facilitate interference in free elections.[15]

Legislative action to protect individuals from privacy violations by the private sector have so far stalled. Enactment of a narrow uniform data breach notification requirement, much less to advance comprehensive privacy legislation, lagged for decades as other nations around the world continue to pass modern privacy protections. Instead, the U.S. operates without comprehensive privacy legislation, relying instead on a patchwork of sectoral laws. The current mix of sectoral regulation and self-regulation is ineffective, inefficient, cumbersome, and costly.

The need for an effective, independent data protection enforcement has likewise never been greater. However, U.S. also still lacks a central data protection agency, hampering its ability to respond to today's vast challenges for data protection. Virtually every other advanced economy recognized the need for an independent agency to address the challenges of the digital age.[16] Compounding the problem, federal agencies with jurisdiction over narrow aspects of privacy protection also often lack sufficient lack sufficient authority and resources. The Federal Trade Commission, the primary U.S. federal agency empowered narrow privacy enforcement provisions does not enforce a general data protection law. The FTC only has authority to bring enforcement actions against unfair and deceptive practices in the marketplace, and it lacks the ability to create prospective rules for data security.[17] The FTC lacks the ability, authority and expertise to engage today's broad range of challenges – Internet of Things, AI, connected vehicles, and more.[18] An independent agency dedicated to data protection could more effectively utilize its resources to police the current widespread exploitation of consumers' personal information.

FTC's failure to enforce a key legal judgment against Facebook is the latest evidence of the U.S. failure act to protect privacy rights; disclosure of the personal data of 50 million users by Facebook to data mining firm Cambridge Analytica that sought to influence the 2016 presidential election.[19] The unlawful disclosure of user records to the data mining firm violated a 2011 FTC

---

[14] For a case study in the extent of private sector location tracking today, *see* Jennifer Valentino-DeVries, Natasha Singer, Michael H. Heller, and Aaron Krolik, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. Times (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-

[15] EPIC, In re Facebook - Cambridge Analytica, Epic.org, https://epic.org/privacy/facebook/cambridge-analytica/.

[16] *See* Letter from EPIC to Sen. Roger Wicker, Chairman, and Sen. Brian Schatz, Ranking Member, S. Comm, on Commerce Sci. & Transp. (July 30, 2018), https://epic.org/testimony/congress/EPIC-SCOM-InternetGovernance-July2018.pdf.

[17] 15 U.S.C. Sec. 45(a)(1).

[18] Comments of EPIC to the Nat'l Telecomm. Info. Admin. on International Internet Policy Priorities 2 (July 31, 2018), https://epic.org/apa/comments/EPIC-NTIA-International-July2018.pdf.

[19] 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-

Consent Order against Facebook that resulted from a sustained campaign by EPIC and other U.S. privacy organizations.[20] This order limited such third-party disclosures, and proper enforcement by the FTC would have prevented the scandal.[21] After the Cambridge Analytica scandal became public, the FTC announced it would reopen the investigation of Facebook. However, nine months have passed since the FTC's announcement of the investigation in March 2018, but the FTC has not issued a judgment, report, or public statement. Meanwhile, the UK ICO promptly issued a report and the maximum fine.[22]

A modern privacy regime would also include "algorithmic transparency" to ensure that key algorithmic decisions made about individuals are clear, justifiable, and fair. For instance, the EU's General Data Protection Regulation[23] and the modernized Council of Europe Privacy Convention[24] both include provisions on algorithmic transparency and accountability. EPIC has also recommended legislative solutions based on the Universal Guidelines for Artificial Intelligence (UGAI).[25] "[I]ntended to maximize the benefits of AI, to minimize the risk, and to ensure the protection of human rights," these guidelines have been signed by over 200 experts and 50 NGOs. However, without government intervention, Google was free to change its search algorithms on YouTube to favor its own content[26] and the scoring of young athletes - even those under 13 - was hidden behind proprietary algorithms.[27]

I. II. Relevant United Nations History and Materials

Including an inquiry about adequacy of U.S. protection of privacy rights from interference by non-state actors in the list of issues prior to reporting by the U.S. would represent a significant first step. While the Human Rights Committee recommendations in 2006 and 2014 United States

---

campaign.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news.

[20] 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 from EPIC to Acting FTC Chair Maureen Ohlhausen (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.

[21] Letter from EPIC, et. al, to Acting FTC Chair Maureen Ohlhausen & Commissioner Terrell McSweeney (Mar. 20, 2018), https://epic.org/privacy/facebook/EPIC-et-al-ltr-FTC-Cambridge-FB-03-20-18.pdf.

[22] *See* Press Release, ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information (Oct. 25, 2018), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/10/facebook-issued-with-maximum-500-000-fine/.

[23] Regulation 2016/679, 2016 O.J. (L119) 1 (EU).

[24] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, ETS No. 108.

[25] Universal Guidelines for Artificial Intelligence (2018), https://thepublicvoice.org/AI-universal-guidelines/.

[26] Letter from EPIC to Commissioners of the Federal Trade Commission (Sept. 8, 2011), https://epic.org/privacy/ftc/google/Google_FTC_Ltr_09_08_11.pdf.

[27] EPIC, In the Matter of Universal Tennis, (Complaint, Request for Investigation, Injunction, and Other Relief) (May 17, 2017), https://epic.org/algorithmic-transparency/EPIC-FTC-UTRComplaint.pdf.

included questions on Article 17, they only touched on national security surveillance authorities, not private sector surveillance.[28] However, significant and growing attention paid to the issue by U.N. Special Rapporteurs, the U.N. High Commissioner for Human Rights, and Human Rights Committee General Comments reflects the need to review Article 17 obligations concerning non-state actors.

The positive obligation of states to protect human rights is well understood. As stated by U.N. Special Rapporteurs:

> State responsibility for human rights can be examined at three levels: The obligation to respect, the obligation to protect, and the obligation to fulfil human rights…The obligation to protect requires from the State and its agents the measures necessary to prevent other individuals or groups from violating the integrity, freedom of action, or other human rights of the individual…[29]

The particular need for governments protect *privacy rights* from interference by non-state actors is self-evident in today's technological landscape. Indeed, the most recent Office of the United Nations High Commissioner for Human Rights (OHCHR) report to the Human Rights Committee in 2018 opened with the following statement: "Driven mostly by the private sector, digital technologies that continually exploit data linked to people's lives, are progressively penetrating the social, cultural, economic and political fabric of modern societies."[30] The state obligation includes "'positive' measures to protect the enjoyment of rights," the OHCHR continued:

> In the context of the right to privacy, that means that implies a duty to adopt legislative and other measures to give effect to the prohibition of and protection against unlawful or arbitrary interference and attacks, whether they emanate from State authorities or from natural or legal persons[31]

This duty is reflected in the OHCHR's Guiding Principles on Business and Human Rights which detailed a "State Duty to Protect Human Rights" in business enterprise context.[32]

---

[28] U.N. Human Rights Comm., *Concluding observations on the fourth periodic report of the United States of America*, ¶ 21, CCPR/C/USA/CO/3/Rev.1 (Dec. 18, 2006). Human Rights Committee, Concluding observations on the fourth periodic report of the United States of America, ¶ 22, CCPR/C/USA/CO/4 (April 23, 2014).
[29] Special Rapporteur Asbjorn Eide, *Report on the right to adequate food as a human right*, ¶¶ 66-69, U.N. Doc. E/CN.4/Sub.2/1987/23 (July 7, 1987). *See also* Special Rapporteur Margaret Sekaggya, *Report of the Special Rapporteur on the situation of human rights defenders*, U.N. Doc. A/65/223 (Aug. 4, 2010).
[30] Office of U.N. High Comm'r for Human Rights, *Report on the right to privacy in the digital age*, ¶ 1 U.N. Doc A/HRC/39/29 (Aug. 3, 2018).
[31] Id. ¶ 24.
[32] Office of U.N. High Comm'r for Human Rights, Guiding Principles on Business and Human Rights (2011), https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

In the "stakeholder contribution" to the OHCHR's landmark 2014 report on the right to privacy in the digital age,[33] the United States notes the ICCPR applies to governmental action but also "recognized the impact that companies and other non-state actors can have on one's privacy, particularly in the digital age."[34] The United States then included what it found to be relevant private sector developments, most notably a 2012 White House proposal for "Consumer Data Privacy in a Networked World."[35]

Perhaps most importantly, the Human Rights Committee also clarified the scope of state responsibility in General Comment 16 on Article 17 that "this right is required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons. "[36] The Committee also powerfully framed state data protection responsibilities:

> The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant.[37]

II. III. Suggested Questions and Recommendations by the Human Rights Committee for the United States

Suggested questions

- We urge the Human Rights Committee to ask the U.S. to clarify the its understanding of the scope of applicability of Article 17 with respect to non-state actors.

- We suggest the Committee ask the U.S. to comment on any measures adopted to ensure that interference with privacy by non-state actors is not arbitrary or unlawful.

---

[33] Office of U.N. High Comm'r for Human Rights, *Report on the right to privacy in the digital age*, U.N. Doc A/HRC/27/37 (June 30, 2014).
[34] United States Response to OHCHR Questionnaire on "The Right to Privacy in the Digital Age" (2014), https://www.ohchr.org/Documents/Issues/Privacy/United%20States.pdf.
[35] White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (2012), https://www.hsdl.org/?view&did=700959 The proposal was never meaningfully debated or passed by Congress.
[36] U.N. Human Rights Comm. *General Comment No. 16 Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation)*, ¶ 1, U.N. Doc. HRI/GEN/1/Rev.9 (Vol. I) (April 8, 1988).
[37] *Id.* ¶ 10.

Suggested recommendations

- We suggest the Human Rights Committee recommend that the U.S. enact a comprehensive privacy law governing non-state actors.

- We suggest the Human Rights Committee recommend that the U.S. create a data protection authority.

IV. Conclusion

EPIC welcomes a close review of United States compliance with the ICCPR, particularly Article 17, by the Human Rights Committee. The fundamental rights of U.S. residents are at issue. We look forward to release of the list of issues prior to reporting.

Sincerely,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President

/s/ Eleni Kyriakides
Eleni Kyriakides
EPIC International Counsel