epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

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

October 3, 2019
United Nations Human Rights Council
Avenue de la Paix 8-14
1211 Genève
Switzerland

Re: Third Universal Periodic Review Cycle, United States of America

Dear United Nations Human Rights Council:

The Electronic Privacy Information Center (EPIC) writes to you regarding the upcoming Universal Periodic Review ("UPR")of the United States by the Human Rights Council ("UNHRC") of the U.S. human rights record.[1] EPIC seeks to provide the UNHRC with information on implementation of the recommendations related to the fundamental right to privacy (UDHR Article 12, ICCPR Article 17). In EPIC's assessment, the U.S. lacks meaningful privacy enforcement, a comprehensive data privacy law, and has failed to curtail mass surveillance of U.S. and non-U.S. persons. EPIC respectfully refers the UNHRC to the annexed report for a comprehensive overview of data privacy developments in the U.S. We note that in the 2015 UPR review, the Working Group called on the United States to respect and protect the right to privacy of persons around the world, to limit surveillance, and to establish new safeguards.[2]

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.[3] EPIC frequently testifies before the U.S. Congress,[4] participates in the U.S. administrative agency rulemaking process,[5] and litigates landmark privacy cases.[6] 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.[7] We have also recently published the *EPIC AI Policy Sourcebook* to provide the basic texts in the AI policy field.[8] EPIC submitted comments to the latest periodic review of U.S. compliance with the International Convention on Civil and Political

[1] UN Human Rights Council, *3rd UPR cycle: contributions and participation of "other stakeholders" in the UPR*, Ohchr.org, https://www.ohchr.org/EN/HRBodies/UPR/Pages/NgosNhris.aspx
[2] Rep. of the Working Group on the Universal Periodic Reviewm United States of America, A/HRC/30/12 (2015) (recommendations #293-305), https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/159/71/PDF/G1515971.pdf?OpenElement.
[3] *See* EPIC, *About EPIC*, https://epic.org/epic/about.html.
[4] EPIC, *EPIC Congressional Testimony and Statements*, EPIC.org, https://epic.org/testimony/congress/.
[5] EPIC, *EPIC Administrative Procedure Act (APA) Comments*, EPIC.org, https://epic.org/apa/comments/.
[6] EPIC, *Litigation Docket*, EPIC.org, https://epic.org/apa/comments/ https://epic.org/privacy/litigation/#cases.
[7] 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/.
[8] EPIC AI Policy Sourcebook (2019), https://epic.org/bookstore/ai2019/.

Rights (ICCPR) by the U.N. Human Rights Committee explaining the U.S. government's failure to protect individuals from privacy interferences by the private sector.[9]

The U.S. has Failed to Protect the Fundamental Right to Privacy with Respect to Private Sector Data Collection, Storage, and Use

1. States have a duty to protect individuals against human rights violations by nonstate actors. Yet the United States has failed to protect the right to privacy with respect to private sector data collection and use. Despite record-breaking data breaches, identity theft, and extensive corporate tracking, the U.S still lacks both a data protection authority and comprehensive privacy legislation

U.S. Operates Without Data Protection Agency

2. Weak enforcement by the Federal Trade Commission, the U.S. administrative agency with jurisdiction over unfair and deceptive trade practices, has failed to enforce basic data protection obligations for the collection and use of personal data. The FTC recently issued settlements with two tech companies which resulted in substantial fines, but these settlements do not include require meaningful changes in business practices or in the collection, use, and dissemination of personal data.

3. For example, the FTC settlement resulting from the unlawful disclosure of user records to Cambridge-Analytica, a firm seeking to influence U.S. and U.K. elections, broadly immunizes Facebook and its officers and directors to violations of the Commission's 2012 Order prior to June 12, 2019 and primarily requires *internal reporting* for the company.[10] EPIC has filed a Motion to Intervene in *United States v. Facebook* charging that the settlement "is not adequate, reasonable, or appropriate."[11] Similarly, the FTC found Google/YouTube knew or should have known it was violating U.S. children's privacy law by targeting ads for children.[12] Nonetheless, the FTC settlement does not require the company to verify channel owners' assertions that they do not market to children and need not comply with children's privacy rules.

U.S. Operates Without Comprehensive Privacy Legislation

4. While the need for a comprehensive privacy law has never been greater, the U.S. also lacks federal baseline legislation. In 2018, the number of consumer records exposed in data breaches

[9] Submission of EPIC to UN Human Rights Committee on List of Issues Prior to Reporting by U.S. (Jan. 10, 2019), https://epic.org/privacy/intl/EPIC-HRC-list-of-issues-20190110.pdf.
[10] Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief, *United States v. Facebook, Inc.*, No. 19-cv-2184 (D.D.C. July 24, 2019).
[11] EPIC, *Challenge to FTC/Facebook 2019 Settlement*, Epic.org, https://epic.org/privacy/facebook/epic2019-challenge/.
[12] Press Release, Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law (Sept. 4, 2019), https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations.

skyrocketed to 446.5 million, an increase of 126% since 2017.[13] Identity fraud is consistently reported. as a top consumer concern by the FTC.[14] The new Congress convened in 2019 has held hearings on privacy concerns. However, there is little progress toward legislative enactment.

5. EPIC released a detailed analysis of the proposals - *Grading on a Curve: Privacy Legislation in the 116th Congress*.[15] EPIC found many of the bills in Congress lack the basic elements of a privacy law, such as an opportunity for individuals to enforce their rights and a proposal to create a data protection agency.

U.S. Foreign Intelligence Surveillance Rises to an Arbitrary or Unlawful Interference with the Fundamental Right to Privacy

6. U.S. law does not prevent arbitrary or unlawful interference with the fundamental right to privacy in conducting foreign intelligence surveillance. Wide ranging surveillance continues under the Foreign Intelligence Surveillance Act Sections 213 and 702, and Executive Order 12333. EPIC does not here not discuss President issued Presidential Policy Directive-28, a presidential order governing surveillance of non-U.S. persons, which featured in the 2015 UPR and has remained unchanged since that review.

Section 215 Call Detail Record Collection Sees Compliance Violations

7. Section 215 of the Foreign Intelligence Surveillance Act authorizes the suspicionless bulk collection of call detail phone records from U.S. telephone companies.[16] The law will expire at the end of 2019 if Congress takes no action, and Congress is currently debating reauthorization. In 2015 after the last Universal Periodic Review, Congress enacted the USA Freedom Act to limit the duration and scope of collection - the statute allows renewable daily production of call metadata records for 180 days, among other requirements collection must correspond to a specific selection term like a phone number.[17]

8. Since the changes were enacted, the 215 program has been the subject of multiple documented compliance violations by the NSA. In June 2018, the NSA announced it collected unauthorized call detail records.[18] The agency was unable to identify the unauthorized records from those which were legitimately collected and was advised to purge all the records collected since

[13] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report* (2018), https://www.idtheftcenter.org/2018-end-of-year-data-breach-report/.
[14] Press Release, Imposter Scams Top Complaints Made to FTC in 2018 (Feb. 28, 2019), https://www.ftc.gov/news-events/press-releases/2019/02/imposter-scams-top-complaints-made-ftc2018.
[15] EPIC, *Grading on a Curve: Privacy Legislation in the 116th Congress* (Sept. 2019), https://www.epic.org/GradingOnACurve.pdf.
[16] 50 U.S.C. § 1861.
[17] *Id*. § 1861(b)(2)(C), (c)(2)(F)(i-ii)
[18] Office of the Director of National Intelligence, *NSA Reports Data Deletion*, IC on the Record (June 28, 2018), https://www.nsa.gov/news-features/press-room/Article/1618691/nsa-reports-data-deletion/.

2015.[19] And, while the agency stated the source of the compliance issue was resolved, a subsequent compliance incident was recently revealed in litigation.[20] The NSA suspended the program indefinitely,[21] but the U.S. administration is now seeking permanent reauthorization of the program.[22]

Section 702 and EO 12333 Surveillance of Electronic Communications Contents Unchanged

9. By contrast, the USA Freedom Act did not reign in foreign intelligence surveillance under Section 702 of FISA. Section 702 of FISA permits broad, "programmatic" surveillance of the communications of non-U.S. persons located outside the U.S, without a requirement to demonstrate probable cause or judicial oversight of individualized surveillance orders.[23] In 2017, U.S. Congress voted to extend Section 702 for another six years.[24] While the intelligence community voluntarily terminated "about" collection[25] - a broad form of collection involving surveillance of communications in which a "selector" like email address is in the body of a communication as opposed to the addressing information[26] - Congress expressly authorized U.S. intelligence agencies to restart "about" collection.[27]

10. Executive Order 12333 surveillance has also not been curtailed since the 2015 UPR.[28] EO 12333 is a Presidential Order governing activities of the U.S. Intelligence Community, and provides broad authority to conduct signals intelligence surveillance for "foreign intelligence and counterintelligence purposes," with few substantive limits on collection.[29] EO 12333 is the primary order under which the NSA conducts foreign intelligence surveillance.[30] Nonetheless, there have been no public reports or significant public disclosures concerning EO 12333 that

---

[19] *Id*.
[20] *NSA FOIA Documents – Quarterly Reports to the Intelligence Oversight Board on NSA Activities*, Aclu.org, https://www.aclu.org/legal-document/nsa-foia-documents-quarterly-reports-intelligence-oversight-board-nsa-activities.
[21] Letter from DNI Daniel Coats to Senate Comms. on Judiciary & Intelligence (Aug. 14, 2019), https://int.nyt.com/data/documenthelper/1640-odni-letter-to-congress-about/20bfc7d1223dba027e55/optimized/full.pdf#page=1.
[22] *Id*.
[23] EPIC, *Foreign Intelligence Surveillance Act (FISA)*, Epic.org https://epic.org/privacy/surveillance/fisa/.
[24] The FISA Amendment Reauthorization Act of 2018, Public Law No: 115-118, 132 Stat. 3 (2018).
[25] See also Press release, NSA Stops Certain Section 702 "Upstream" Activities (April 28, 2017). See https://www.nsa.gov/news-features/press-room/statements/2017-04-28-702-statement.shtml.
[26] PCLOB, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 7 (2014).
[27] Public Law No: 115-118, 132 Stat. 3 (2018)
[28] 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).
[29] EO 12333 § 1.7(c)(1).
[30] See *Data Protection Commissioner v. Facebook Ireland and Schrems*, Judgment of 3rd October 2017, at para. 175, https://www.dataprotection.ie/sites/default/files/uploads/2019-07/High%20Court%20Judgment_Updated%2012.04.2018.pdf.

describe how these programs operate, before the 2015 UPR or after; EO 12333 is not subject to judicial oversight and no legal remedy for NSA surveillance is available.[31]

Conclusion

11. We ask that this submission EPIC be considered in the universal periodic review of the U.S. EPIC looks forward to the concluding report and recommendations of the UNHRC.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Eleni Kyriakides*
Eleni Kyriakides
EPIC International Counsel

[31] *Id*.