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

to the
EUROPEAN COMMISSION
Privacy Shield Third Annual Review

July 15, 2019

The Electronic Privacy Information Center ("EPIC") submits the following comments to the European Commission, pursuant to a request from the Directorate-General for Justice and Consumers / International Data Flows and Protection for comments from EPIC for the third annual review of the EU- U.S. Privacy Shield.[1] Since the 2018 review, the U.S. still operates without the basic privacy guarantees of comprehensive privacy legislation or an independent data protection authority. And while EPIC welcomes positive developments in artificial intelligence policy and appointments to the Privacy and Civil Liberties Oversight Board, the bulk surveillance of non-U.S. persons is still authorized under U.S. law (Section 702). The U.S. has also expanded invasive border surveillance techniques, such as facial recognition for travelers entering and exiting the United States and social media data collection for visa applicants.

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 the Congress,[3] participates in the administrative agency rulemaking process, [4] and litigates landmark privacy cases.[5]

---

[1] EPIC, *Privacy Shield EU-U.S. Data Transfer Arrangement*, Epic.org, https://www.epic.org/privacy/intl/privacy-shield/.
[2] *See*, EPIC, *About EPIC,* EPIC.org, *https://epic.org/epic/about.html.*
[3] EPIC, *EPIC Congressional Testimony and Statements,* EPIC.org, https://epic.org/testimony/congress/.
[4] EPIC, *EPIC Administrative Procedure Act (APA) Comments,* EPIC.org, https://epic.org/apa/comments/.
[5] EPIC, *Litigation Docket,* EPIC.org, https://epic.org/apa/comments/ https://epic.org/privacy/litigation/#cases.

EPIC's Interest

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.[6] EPIC 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 laws and international frameworks.[7] EPIC also provides semi-annual U.S. country reports to the International Working Group on Data Protection.[8]

EPIC has a long history of evaluating proposals for trans-Atlantic data flows. EPIC has supported strong international frameworks for data protection and called for U.S. ratification of Council of Europe Convention 108.[9] EPIC and a coalition of EU and U.S. consumer organizations also criticized the Privacy Shield prior to adoption for its failure to comply with the terms set out by the Court of Justice for the European Union ("CJEU") in its Safe Harbor Decision."[10] EPIC President Marc Rotenberg outlined the shortcomings in Safe Harbor protection in testimony before the European Parliament[11] and U.S. Congress.[12] And after serving as the sole U.S. NGO *amicus* in national court, EPIC is a party to *Data Protection Commissioner v. Facebook* - an Irish case referred to the CJEU concerning the validity of the "standard contractual clauses" for transfer of EU consumers' data to the U.S., heard by the court on July 9th.[13] EPIC has long made clear its support for comprehensive, meaningful, and effective legal protections for personal data.

---

[6] *See*, *About the Public Voice*, The Public Voice, http://thepublicvoice.org/about-us/.
[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 2016: United States Law, International Law, and Recent Developments* (ed. M. Rotenberg EPIC 2018), available at: https://epic.org/bookstore/.
[8] *See, e.g.*, EPIC, International Working Group on Data Protection in Telecommunications 65th Meeting Bled, Slovenia – 9-10 April 2019, Country Report United States of America (provided by EPIC) (2019), https://epic.org/IWG/IWG65-EPIC-Report.pdf.
[9] *See, e.g.*, Letter from EPIC to Senate Comm. on Foreign Relations (Apr. 13, 2018), https://www.epic.org/EPIC-SFR-Pompeo-April2018.pdf.
[10] Letter from EPIC, et. al, to Article 29 Working Party (Mar. 16, 2016), https://epic.org/privacy/intl/schrems/Priv-Shield-Coalition-LtrMar2016.pdf; EPIC, *Max Schrems v. Data Protection Commissioner (CJEU - "Safe Harbor")*, Epic.org, https://epic.org/privacy/intl/schrems/.
[11] Testimony and Statement of Marc Rotenberg, EPIC President, The Reform of the EU Data Protection Framework— Building Trust in a Digital and Global World Before the Comm. of the European Parliament on Civil Liberties, Justice, & Home Affairs, European Parliament (Oct. 10, 2012), https://www.epic.org/privacy/Rotenberg_EP_Testimony_10_10_12.pdf.
[12] Testimony and Statement of Marc Rotenberg, EPIC President, Examining the EU Safe Harbor Decision and Impacts for Transatlantic Data Flows: J, Hearing Before H. Energy & Commerce Subcomm, on Commerce, Manufacturing, Trade, Comm'n & Tech. (Nov. 3, 2015), https://epic.org/privacy/intl/schrems/EPIC-EU-SH-Testimony-HCEC-11-3-final.pdf.
[13] EPIC, *Data Protection Commissioner v. Facebook & Max Schrems (CJEU)*, Epic.org, https://epic.org/privacy/intl/DPC-v-Facebook-CJEU/.

We appreciate the opportunity to provide input into the European Commission's third annual review of the EU-U.S. Privacy Shield. The Commission requested information concerning developments since October 2018 that are relevant to the assessment of the Privacy Shield. Accordingly, Part I provides updates on U.S. surveillance and law enforcement access to personal data, Part II on U.S. consumer privacy protection, and Part III on U.S. policy on Artificial Intelligence and automated decision-making. Finally, Part IV discusses additional developments relevant to U.S. obligations under Privacy Shield.

The Privacy Shield

The Privacy Shield aimed to replace the Safe Harbor framework for commercial data flows between the EU and the U.S., struck down by the Court of Justice of the European Union in October 2015. The Privacy Shield includes added protections consumer data transferred under the agreement and a set of assurances about U.S. surveillance.[14]

For many years, EPIC supported establishment of a comprehensive privacy framework in the United States and limits on surveillance to enable stable transborder data flows.[15] EPIC previously urged that the United States begin the process of ratification of Council of Europe Convention 108.[16] EPIC also launched "Data Protection 2016" to support stronger privacy safeguards in the US.[17]

When the Privacy Shield was proposed, however, in letter to Commissioner Vera Jourova and Secretary Penny Pritzker, EPIC and more than 40 NGOs urged the U.S. and the EU to protect the fundamental right to privacy.[18] The groups warned that that without significant changes to "domestic law" and "international commitments," a new framework would almost certainly fail. EPIC and a coalition of NGOs also called on the European Union, including the Article 29 Working Party to oppose the Privacy Shield for the failure to meet the requirements of the European Court of Justice in the *Schrems* case.[19]

EPIC President Marc Rotenberg testified to the LIBE Committee of the European Parliament outlined flaws in the Shield, including a weak privacy framework, lack of enforcement, and a cumbersome redress mechanism.[20] Rotenberg recommended that the EU condition acceptance of the

---

[14] EPIC, Privacy Shield EU-U.S. Data Transfer Arrangement, https://epic.org/privacy/intl/privacy-shield/

[15] The Madrid Privacy Declaration (2009), http://www.thepublicvoice.org/Madrid-declaration/.

[16] *See, e.g.*, Letter from EPIC to Senate Comm. on Foreign Relations, *supra* note 9.

[17] *Data Protection 2016*, http://www.dataprotection2016.org.

[18] Letter from EPIC, et. al, to Dep't of Commerce, European Comm'n (Nov. 13, 2015)), https://thepublicvoice.org/EU-US-NGO-letter-Safe-Harbor-11-15.pdf.

[19] Letter from EPIC, et. al, to Article 29 Working Party, et. al (Mar. 16, 2016), https://epic.org/privacy/intl/schrems/Priv-Shield-Coalition-LtrMar2016.pdf.

[20] *Committee Meeting:: Committee on Civil Liberties, Justice and Home Affairs*, European Parliament, (Mar. 17, 2016), http://www.europarl.europa.eu/ep-live/en/committees/video?event=20160317-1500-COMMITTEE-LIBE.

Privacy Shield on the end of the "702 program," which permits U.S. bulk surveillance of non. U.S. persons located abroad.[21]

II. National Security and Law Enforcement Access to Data

A. No Change to Foreign Intelligence Surveillance Act "Section 702"

Since the 2018 annual review of Privacy Shield, has been no significant change to Section 702 of FISA. Section 702 of FISA permits broad, "programmatic" surveillance of non-U.S. persons located outside the U.S. It contains no requirement to demonstrate probable cause or that a target is engaged in criminal activity and does not require individualized surveillance orders.[22]

In 2017, U.S. Congress voted to extend Section 702 for another six years[23] As noted in EPIC's comments on the second annual review, the reauthorization did not include new privacy protections for non-U.S. persons.[24] Indeed, extending new privacy protections to non-U.S. persons was meaningfully considered during the legislative debate over 702's reauthorization. The reauthorization act also expressly authorized U.S. intelligence agencies to restart "about" collection,, a broad form of collection involving 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."[25] In conducting "about" collection, government access to communications necessarily involves scanning the content of all messages over a particular network in order to find selected terms within the body of a communication.[26] While the NSA ended "about" collection in 2017,[27] the Act authorized the program to be restarted upon notice to Congress.[28]

In June 2019, Reps. Justin Amash (R-Mich.) and Zoe Lofgren (D-Calif.) co-sponsored an amendment to an appropriations bill that would have prevented the government from knowingly collecting domestic communications under 702.[29] While there was significant coverage of the

---

[21] EPIC, *EPIC's Rotenberg Urges European Parliament to Condition "Privacy Shield' on End of 702 Surveillance*, Epic.org (Mar. 17, 2016), https://epic.org/2016/03/epics-rotenberg-urges-european.html.
[22] EPIC, *Foreign Intelligence Surveillance Act (FISA)*, Epic.org https://epic.org/privacy/surveillance/fisa/.
[23] The FISA Amendment Reauthorization Act of 2018, Public Law No: 115-118, 132 Stat. 3 (2018)
[24] EPIC Comments to European Commission on Privacy Shield Second Annual Review (Aug. 14, 2018), https://epic.org/privacy/intl/Comments_Privacy_Shield_Review_2.pdf.
[25] Privacy and Civil Liberties Oversight Bd., Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 7 (2014) [PCLOB 702 Report]
[26] *Id.*
[27] 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.
[28] FISA Amendment Reauthorization Act § 2.
[29] Amendment to Division C of Rules Committee Print 116-17, Labor, Health and Human Services, Education, Defense, State, Foreign Operations, and Energy and Water Development Appropriations

amendment, protections for non-U.S. persons were not meaningfully debated. This amendment failed in a vote on June 18, 2019.[30]

B. Congress Debates Foreign Intelligence Surveillance Act "Section 215", Program Status Unconfirmed

The Patriot Act Section 215 authorizes the broad collection of call detail phone records from U.S. companies.[31] The law will sunset at the end of 2019 if Congress does not reauthorize Section 215. Historically, the U.S. intelligence community relied on the Foreign Intelligence Surveillance Act (FISA) Section 215 program to justify bulk collection of all call metadata created by U.S. companies, a practice ruled unlawful by a U.S. circuit court.[32] In 2015, the USA Freedom Act limited the program.[33] Now the government may request ongoing production of records for 180 days with extension available.[34] Production must be based on a particular phone number or other selection term for which there is reasonable suspicion that the selection term is associated with international terrorism, as approved by the FISA Court.[35] However, the government can still access not only all records of those who communicated with an approved selection term, but also all records of those who communicated with the second set of numbers.[36]

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.[37] 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 2015.[38] And, while the agency stated the root of the compliance issue was resolved, a subsequent compliance incident was recently revealed in litigation.[39]

Act, 2020, H.R. 2740, 116th Cong. (2019), https://amendments-rules.house.gov/amendments/AMASH_041_xml67191043274327.pdf.

[30] Office of the Clerk of the U.S. House of Representatives, Final Vote Results for Roll Call 345, http://clerk.house.gov/evs/2019/roll345.xml.

[31] 50 U.S.C. 1861.

[32] EPIC, *American Civil Liberties Union v. Clapper*, Epic.org, https://epic.org/amicus/fisa/215/aclu/.

[33] Press Release, NSA Reports Data Deletion (June 28, 2018), https://www.nsa.gov/news-features/press-room/Article/1618691/nsa-reports-data-deletion/.

[34] 50 U.S.C §1861(c)(2)(F)(i-ii)..

[35] *Id*. § 1861 (b)(2)(C).

[36] *Id*. §1861(c)(2)(F)(iv).

[37] Office of the Director of National Intelligence, *NSA Reports Data Deletion*, IC on the Records (June 28, 2018).

[38] *Id*.

[39] *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.

The status of the 215 program is also unclear. A Senior Congressional aide acknowledged in a press interview that the National Security Agency ended the call detail record program in 2018.[40] However, the agency has neither confirmed nor denied the reports.[41] Unconfirmed reports also suggest that the NSA recommended the White House not request renewal of the Section 215 phone records program, concluding intelligence benefits do not justify the logistical and legal burdens of keeping it.[42] The Director of the NSA has stated publicly only that the NSA is "in a deliberative process" to determine the future of the Section 215 program.[43]

EPIC and a coalition of civil liberties organizations sent a statement to the House Judiciary Committee calling for a permanent end to the NSA's phone record collection program.[44] The groups called on Congress to "hold hearings and make public information critical to permit an informed debate over the reauthorization of Section 215 and other provisions of the Patriot Act, which are set to expire December 15, 2019." A bipartisan bill to permanently end the call detail record program was also introduced earlier this year.[45]

C. The Privacy and Civil Liberties Oversight Board is Now Operating

In June 2019, the U.S. Senate confirmed three members to the Privacy and Civil Liberties Oversight Board. The confirmation fills the Board's five seats for the first time in several years. The Privacy and Civil Liberties Oversight Board provides oversight and advice over executive branch intelligence activities.[46]

---

[40] Charlie Savage, *Disputed N.S.A. Phone Program Is Shut Down, Aide Says,* N.Y. Times (Mar. 4, 2019), https://www.nytimes.com/2019/03/04/us/politics/nsa-phone-records-program-shut-down.html; Jen Patja Howell, *The Lawfare Podcast: Luke Murry and Daniel Silverberg on National Security in Congress*, Lawfare (Mar. 2, 2019), https://www.lawfareblog.com/lawfare-podcast-luke-murry-and-daniel-silverberg-national-security-congress.

[41] *Id.*

[42] Dustin Volz and Warren P. Strobel, *NSA Recommends Dropping Phone-Surveillance Program*, The Wall Street Journal (April 24, 2019), https://www.wsj.com/articles/nsa-recommends-dropping-phone-surveillance-program-11556138247.

[43] Dustin Volz, *NSA in 'Deliberative Process' Over Metadata Surveillance, Its Chief Says* (Mar. 6, 2019), https://www.wsj.com/articles/nsa-in-deliberative-process-over-metadata-surveillance-chief-says-11551913327.

[44] Letter from EPIC, et. al, to , House Comm. on the Judiciary (Mar. 18, 2019), https://epic.org/privacy/nsa/EPIC-Letter-to-House-Judiciary-re-NSA-bulk-surveillance-03182019.pdf.

[45] Ending Mass Collection of Americans' Phone Records Act of 2019, 116th Cong. (2019), https://www.wyden.senate.gov/imo/media/doc/Ending%20Mass%20Collections%20of%20Americans'%20Phone%20Records%20Act%20of%202019%20Bill%20Text.pdf.

[46] PCLOB, *History and Mission*, Pclob.gov, https://www.pclob.gov/about/.

The Board held its first public meeting in February 2019 on "Countering Terrorism while Protecting Privacy and Civil Liberties: Where do We Stand in 2019."[47] While the Board has not released a public report, several new oversight projects were announced. The PCLOB reviews federal agency programs to ensure they do not diminish privacy and civil liberties. The Board has announced new reviews of: (1) the use of biometrics, such as facial recognition, in airports; (2) how the FBI queries data collected under the Foreign Intelligence Surveillance Act's Section 702, including searches for US person information called "backdoor searches"; (3) oversight of passenger identity databases used by airlines; and (4) the reforms of the domestic call detail record program initiated by the 2015 USA Freedom Act.[48]

Board has also published an inventory of current oversight activities.[49] Notably, the Board announced it is reviewing NSA's search tool called "xkeyscore." The tool is used to search data collected under Executive Order 12333, the primary legal authority for foreign intelligence surveillance. This presidential order not yet been subject to public oversight or public reports. The Board will also issue a public report on how the intelligence community is implementing reforms of the Section 702 programs proposed by the Board in 2014.[50]

When the Board reached quorum, EPIC sent a statement to the Board outlining priorities proposing several oversight projects. EPIC said the Civil Liberties Board should (1) release the report on Executive Order 12333; (2) limit government use of facial recognition; (3) establish safeguard for government AI use; (4) monitor proposals for "smart" borders and assess privacy impacts on US residents; and (5) reform Section 702 surveillance authority.[51] Several of these projects are now underway by the Board. EPIC previously testified before PCLOB to set out a broad agenda for the work of the independent agency, and spoke at the first meeting of the Oversight Board in 2013.[52]

---

[47] Press Release, Privacy and Civil Liberties Oversight Board Announces Panelists for Upcoming Public Forum (Jan. 30, 2019), https://www.pclob.gov/newsroom/20190130.html.
[48] Press Release, "From Booking to Baggage Claim:" Privacy and Civil Liberties Oversight Board to Examine Use of Facial Recognition and Other Biometric Technologies in Aviation Security (June 26, 2019), https://epic.org/privacy/PLCOB/Press-release-june262019.png.
[49] Privacy & Civil Liberties Oversight Board, Active Oversight Projects & Other Engagements (2019), https://epic.org/privacy/PLCOB/AgendaJuly2019.pdf.
[50] Privacy & Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (2014), https://www.pclob.gov/library/702-Report.pdf.
[51] Letter from EPIC to Privacy & Civil Liberties Oversight Bd. (Feb. 7, 2019), https://epic.org/testimony/congress/EPIC-PCLOB-Feb2019.pdf.
[52] Marc Rotenberg, *Prepared Statement for the Record, Workshop on "Domestic Surveillance Programs Operated Under the USA PATRIOT Act and the Foreign Intelligence Surveillance Act" Before the Privacy and Civil Liberties Oversight Board*, Epic.org (July 9, 2013), https://epic.org/privacy/oversight/EPIC-PCLOB-Statement.pdf; Statement of EPIC to the Privacy and Civil Liberties Oversight Board on "Sunshine Act; Notice of Meeting" (Oct. 23, 2012), https://epic.org/privacy/1974act/EPIC-PCLOB-Statement-10-12.pdf.

E. Privacy Shield Ombudsperson Appointed

On June 20, 2019, the U.S. Senate confirmed Keith Krach to serve as Under Secretary of State for Economic Growth, Energy, and the Environment[53] – the official designated to serve as the EU-U.S. Privacy Shield Ombudsperson.[54] Mr. Krach is Chairman and former CEO of an e-signature company DocuSign. He was simultaneously confirmed for several other positions: United States Alternate Governor of the European Bank for Reconstruction and Development, United States Alternate Governor of the International Bank for Reconstruction and Development, and the United States Alternate Governor of the Inter-American Development Bank for a term of five years.[55]

EPIC sent a letter to the Senate regarding the nomination of Mr. Krach to underscore the urgency of updating federal privacy law, establishing a data protection agency in the United States, and ratifying Council of Europe Convention 108.[56] EPIC further explained to the United States Senate that the Privacy Shield is not an effective basis for EU-US data flows:

> Without more substantial reforms to ensure protection for fundamental rights of individuals on both sides of the Atlantic, Privacy Shield will put users at risk and undermine trust in the digital economy. Specifically, the United States must commit to protecting the data privacy of both US-persons and non-US-persons in order to protect users and instill trust in the digital economy.[57]

II. Consumer Privacy Protection

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

The need for U.S. comprehensive privacy legislation, enforced by a data protection agency, in the U.S has never been greater. In 2018, the number of consumer records exposed in data breaches skyrocketed to 446.5 million, an increase of 126% since 2017.[58] Identity fraud is consistently reported

---

[53] Press Release, President Donald J. Trump Announces Intent to Nominate Individual to Key Administration Posts (Jan. 18, 2019), https://www.whitehouse.gov/presidential-actions/president-donald-j-trump-announces-intent-nominate-individual-key-administration-posts/; *Senate Floor Activity - Thursday, June 20, 2019*, Senate.gov (June 20, 2019), https://www.senate.gov/legislative/LIS/floor_activity/06_20_2019_Senate_Floor.htm.

[54] *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.

[55] *Senate Floor Activity - Thursday, June 20, 2019*, *supra* note 53.

[56] Letter from EPIC to Senate Comm. on Foreign Relations (Mar. 26, 2019), https://epic.org/testimony/congress/EPIC-SFR-KeithKrach-Mar2019.pdf.

[57] *Id. citing* Letter from EPIC, et al., to Article 29 Working Party, et al. (Mar. 16, 2016), https://epic.org/privacy/intl/schrems/Priv-Shield-Coalition-LtrMar2016.pdf.

[58] Identity Theft Resource Center, 2018 End-of-Year Data Breach Report (2018), https://www.idtheftcenter.org/2018-end-of-year-data-breach-report/.

as a top consumer concern by the FTC.[59] The new Congress convened in 2019 has begun to hold hearings on U.S. federal privacy legislation. However, there has yet to be a vote on federal privacy legislation in either the House or Senate.

The new Congress convened in 2019 has begun to hold hearings on U.S. federal privacy legislation. Significant hearings included House Commerce Committee hearing on "Protecting Consumers in the Era of Big Data," a Senate Commerce hearings on "Policy Principles for a Federal Data Privacy Framework in the United States" and "Consumer Perspectives: Policy Principles for a Federal Data Privacy Framework," Senate Judiciary hearings on "GDPR & CCPA: Opt-ins, Consumer Control, and the Impact on Competition and Innovation" and "Online Platforms and Market Power," and a Senate Commerce Hearing on "Small Business Perspectives on a Federal Data Privacy Framework." Key questions emerging in the US debate over a federal privacy law are whether a federal law should preempt state laws, such as the recently enacted California Consumer Protection Act, and the need for a federal data protection authority, discussed further below. [60]

Simultaneously, the Federal Trade Commission held over a dozen public hearings on Competition and Consumer Protection in the 21st Century. The hearings examine "whether broad-based changes in the economy, evolving business practices, new technologies, or international developments might require adjustments to competition and consumer protection law, enforcement priorities, and policy."[61] EPIC Consumer Protection Christine Bannan of EPIC testified to the need for a federal data protection authority.[62] However, there has also not yet been a concrete outcome of the hearings.

Consumer groups, including EPIC, have endorsed a policy framework for federal privacy legislation based on eight goals: (1) enact baseline federal legislation; (2) enforce fair information practices; (3) establish a data protection agency; (4) ensure robust enforcement; (5) establish algorithmic governance; (6) prohibit "take it or leave it" terms; (7) promote privacy innovation; and (8) limit government access to personal data.[63]

---

[59] 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-ftc-2018.

[60] *See, e.g.*, Letter from EPIC to Senate Commerce Comm. (Mar. 26, 2019), https://epic.org/testimony/congress/EPIC-SCOMSmallBusiness-Mar2019.pdf; Letter from EPIC to Senate Judiciary Comm. (Mar. 11, 2019), https://epic.org/testimony/congress/EPIC-SJC-GDPRandCCPA-Mar2019.pdf; Letter from EPIC to Senate Commerce Comm. (Apr. 29, 2019), https://epic.org/testimony/congress/EPIC-SCOM-ConsumerPerspectives-Apr2019.pdf.

[61] Hearings on Competition and Consumer Protection in the 21st Century, 83 F.R. 38307 (2018).

[62] Transcript of Competition and Consumer Privacy in the 21st Century, Hearing 12.2, Fed, Trade Commission (Apr. 10, 2019), https://www.ftc.gov/system/files/documents/public_events/1418273/ftc_hearings_session_12_transcript_day_2_4-10-19.pdf.

[63] A Framework for Comprehensive Privacy Protection and Digital Rights in the United States (2019), https://www.citizen.org/wp-content/uploads/migration/privacy-and-digital-rights-for-all-framework.pdf.

B. U.S. Sill Without Data Protection Agency as Enforcement Actions Lag

Establishment of a U.S. data protection agency has emerged as a key debate in Congress and at the FTC, alongside comprehensive privacy legislation. The Congress has taken no vote on legislation to create a U.S. DPA. Exemplified by the long-delayed enforcement action on Cambridge Analytica, the FTC has broadly failed to enforce the agency's own consent orders and oversee consumer privacy - even when the FTC reaches a consent agreement with a privacy-violating company, the Commission rarely enforces the Consent Order terms.

FTC took 15 months to bring an enforcement action against Facebook for the disclosure of the personal data of 50 million users to Cambridge Analytica, the controversial British data mining firm that sought to influence the 2016 presidential election and the Brexit Vote. In March 2018, after the Cambridge Analytica scandal became public, the FTC announced it would reopen the investigation of Facebook.[64] The unlawful disclosure of user records to the data mining firm likely violated a 2011 FTC Consent Order against Facebook that resulted from a sustained campaign by US privacy organizations.[65] EPIC and consumer organizations called on the FTC to "immediately undertake an investigation and issue a public report as to whether Facebook complied with the 2011 Order."[66] EPIC joined with Color of Change, the Open Markets Institute and others to urge the FTC to impose a significant fine and to break up the company, reform hiring and management practices, and install a director to represent users.[67] Only a year and a half later, unconfirmed reports suggest the FTC finally settlement with the company in June 2019.[68]

Through a Freedom of Information Act request, EPIC also learned that the FTC has over 25,000 complaints about Facebook pending with the Commission.[69] In the eight years since the FTC announced a Consent Order with Facebook, the FTC had not taken a single enforcement order against

---

[64] Press Release, Statement by the Acting Director FTC 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.

[65] 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.

[66] Letter from EPIC, et. al, to FTC (Mar. 20, 2018), https://epic.org/privacy/facebook/EPIC-et-al-ltr-FTC-Cambridge-FB-03-20-18.pdf.

[67] Letter from EPIC, et. al, to FTC (Jan. 24, 2019), https://epic.org/privacy/facebook/2011-consent-order/US-NGOs-to-FTC-re-FB-Jan-2019.pdf.

[68] Emily Glazer, *FTC Approves Roughly $5 Billion Facebook Settlement*, Wall Street Journal (June 12, 2019), https://www.wsj.com/articles/ftc-approves-roughly-5-billion-facebook-settlement-11562960538?mod=djemalertNEWS.

[69] EPIC, *EPIC FOIA: FTC Confirms More than 25,000 Facebook Complaints are Pending*, Epic.org (Mar. 27, 2019), https://epic.org/2019/03/epic-foia---ftc-confirms-more-.html.

the company. "The FTC is simply ignoring thousands of consumer privacy complaints about Facebook's ongoing business practices," as EPIC said in a recent statement to Congress.[70]

As a result, EPIC made a decision to lobby for the creation a data protection agency in the United States. EPIC's President explained that EPIC had not previously lobbied Congress, but would do so now, stating "we have decided that EPIC can no longer stand on the sidelines."[71] The statement concludes, "A data protection agency is the cornerstone of effective privacy protection. Data protection agencies act as ombudsmen for the public. They encourage innovation and good business practices. They identify emerging privacy challenges and pursue solutions. They take enforcement action when necessary and they impose penalties that are meaningful. Virtually every democratic country has created a privacy agency. But the United States has not. As a consequence, data breach and identity theft continue to rise in the United States. The pace of mergers is accelerating and the rate of innovation is slowing." EPIC has historically testified before Congress numerous times on the need for the U.S. to establish a data protection agency,[72] in addition to submitting letters to Congressional hearings[73] and comments to federal agencies urging the same.[74]

III. Policy Developments for Artificial Intelligence & Automated Decision-Making

A. Executive Order on Artificial Intelligence Released

President Trump signed an "Executive Order on Maintaining American Leadership in Artificial Intelligence" in February 11, 2019.[75] The Order provides a general framework for U.S. AI policy development and forms the basis for subsequent federal requests for comment on granular AI policies and frameworks.

The document focuses heavily on investing resources on research and development resources and coordinating federal activity on AI. However, the Order also cites to the need to foster public confidence and uphold "civil liberties, privacy and American values."[76] To this end, the Order requires

[70] https://epic.org/testimony/congress/EPIC-HEC-FTCOversight-May2019.pdf
[71] Press release, EPIC To Lobby to Establish Data Protection Agency in the United States (June 20, 2019), https://epic.org/press/EPIC-To-Lobby-to-Establish-DPA.pdf
[72] Testimony and Statement of Marc Rotenberg, EPIC President, Hearing on Consumer Data Security and the Credit Bureaus Before the S. Comm. on Banking, Housing, & Urban Affairs United States Senate (Oct. 17, 2018), https://epic.org/privacy/testimony/EPIC-Testimony-SBC-10- 17.pdf
[73] *See, e.g.*, Letter from EPIC to Senate Commerce Comm, *supra* note 60.
[74] Comments of EPIC to FTC on Draft Strategic Plan for Fiscal Years 2018 to 2022 (Dec. 5, 2017), https://epic.org/privacy/ftc/EPIC-Comments-FTC-Draft-Strategic-Plan-12- 05- 17.pdf.
[75] Exec. Order No. 13859, 84 Fed. Reg. 3967 (Feb. 11, 2019), https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/.
[76] *Id.* § 1.

framework for AI governance within the federal government, then implemented by each agency.[77] This document is required to be submitted for public comment before finalized.[78]

Also flowing from the requirements of the Order, the White House is now requesting public comment on which federal data and models should be made available for AI research, development, and testing.[79] The Privacy Act of 1974 imposes limits on how government agencies collect, use, and transfer personal data.[80] EPIC has strongly favored greater use of federal data that is not personally identifiable, such as statistical data and data concerning climate change, but has warned against the use of personal data maintained by federal agencies for AI projects.[81]

B. U.S. Endorses OECD AI Guidelines

The United States endorsed the OECD Council Recommendation on Artificial intelligence, formally adopted at the OECD Council Meeting on May 22-23.[82] The document includes strong principles on fairness, accountability, and transparency, also robustness, security, safety, and inclusive growth. The protection of human rights, the rule of law, and democratic values feature prominently. The G20 Ministers, including the U.S, subsequently adopted AI principles based on the OECD's at the G20 Summit in Osaka, Japan.[83]

EPIC has filed comments with the National Institute of Standards and Technology urging the U.S. to begin to implement the OECD Principles on Artificial Intelligence into binding federal AI policy.[84] EPIC also urged NIST to go further and adopt the Universal Guidelines for Artificial Intelligence. The Universal Guidelines are design reduce bias in decision-making algorithms, ensure digital globalization is inclusive, create human-centered evidence-based policy, promote safety in AI deployment in national security uses, and rebuild trust in institutions.[85] EPIC also said the agency should go further by adopting the Universal Guidelines for AI. Over 250 experts and 60 organizations,

---

[77] *Id*. § 6(a-c).
[78] *Id*. § 6(b).
[79] EPIC, *White House Seeks Public Comments on AI and Federal Data*, Epic.org, (July 11, 2019), https://epic.org/2019/07/white-house-seeks-public-comme.html.
[80] EPIC, *Privacy Act of 1974*, Epic.org, https://epic.org/privacy/1974act/.
[81] Marc Rotenberg, *Let's Use Government Data to Make Better Policy*, Scientific American (Oct. 4, 2017), https://blogs.scientificamerican.com/observations/let-rsquo-s-use-government-data-to-make-better-policy/
[82] *OECD moves forward on developing guidelines for artificial intelligence (AI)*, OECD (Feb. 20, 2019), http://www.oecd.org/going-digital/ai/oecd-moves-forward-on-developing-guidelines-for-artificial-intelligence.htm.
[83] G20 Ministerial Statement on Trade and Digital Economy (2019), https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf.
[84] Comments of EPIC to NIST on Artificial Intelligence Standards (May 31, 2019), https://epic.org/privacy/ai/NIST-RFI-EPIC%2020190531.pdf.
[85] Universal Guidelines for Artificial Intelligence (2018), https://thepublicvoice.org/ai-universal-guidelines/.

representing more than 40 countries have endorsed the UGAI, which are intended to maximize the benefits of AI, to minimize the risk, and to ensure the protection of human rights.

C. White House Updates National AI Research and Development Plan

The White House published the 2019 update of the National Artificial Intelligence Research and Development Strategic Plan.[86] The report sets out priorities for U.S. AI policy. The 2019 report carries forward seven recommendations from the 2016 plan and sets new aims. The plan underscores the need to address the ethical, legal, and societal implications of AI (Strategy #3), emphasizes safety and security (Strategy #4), and the development of standards and benchmarks (Strategy #6). A new recommendation "focuses on the increasing importance of effective partnerships between the Federal Government and academia, industry, other non-Federal entities, and international allies to generate technological breakthroughs in AI."

The 2019 report acknowledges input from "researchers, research organizations, professional societies, civil society organizations and individuals." Common themes included "the importance of developing trustworthy AI systems, including fairness, ethics, accountability, and transparency of AI systems." EPIC—joined by nearly 100 experts and leading scientific organizations including AAAS, ACM, FAS, and IEEE—successfully petitioned the White House Select Committee on Artificial Intelligence to incorporate public input in the committee's work.[87] In part, EPIC recommended that the US AI strategy incorporate the Universal Guidelines for Artificial Intelligence in national policy.[88] As the report notes, "beyond purely data-related issues, however, larger questions arise about the design of AI to be inherently just, fair, transparent, and accountable."

D. National Security Commission on Artificial Intelligence Operates in Secret

A recently established National Security Commission on AI has operated without transparency or public input. The National Security Commission on Artificial Intelligence held its first meeting in March 2019 with no notice of the meeting and no opportunity for public participation.[89] The Commission was created by Congress in the National Defense Authorization Act and is tasked reviewing "advances in artificial intelligence, related machine learning developments, and associated technologies" to support the security and defense of the U.S.[90] Members of the Commission were

---

[86] Select Comm. on Artificial Intelligence, National Artificial Intelligence Research and Development Strategic Plan: 2019 Update (2019), https://www.whitehouse.gov/wp-content/uploads/2019/06/National-AI-Research-and-Development-Strategic-Plan-2019-Update-June-2019.pdf.

[87] Petition to OSTP for Request for Information on Artificial Intelligence Policy (July 4, 2018), https://epic.org/privacy/ai/OSTP-AI-Petition.pdf.

[88] Comments of EPIC to Nat'l Science Found. on Update to the 2016 National Artificial Intelligence Research and Development Strategic Plan (Oct. 26, 2018), https://epic.org/apa/comments/EPIC-Comments-NSF-AI-Strategic-Plan-2018.pdf.

[89] Justin Doubleday, *National Security Commission on AI hosts first meeting*, Inside Defense (Mar. 13, 2019), https://insidedefense.com/insider/national-security-commission-ai-hosts-first-meeting.

[90] P.L. 115-232, Section 2, Division A, Title X, §1051.

chosen by members of Congress and agency heads.[91] In its role the Commission is also required to review ethical considerations of AI.[92]

EPIC is seeking the public release of the documents distributed at the AI Commission meeting.[93] The Commission was also tasked with delivering a public report on February 9, 2019. The report has yet to be released, and the EPIC FOIA also requests that report.[94] " Companies or members of the public interested in learning how the Commission is studying AI are left only with the knowledge that appointed people met to discuss these very topics, did so, and are not yet releasing any information about their recommendations," as one commentator recently wrote.[95]

The Inspector General of the U.S. Intelligence Community recently called for greater oversight of the use of AI by U.S. intelligence agencies.[96] In a semiannual report to Congress, the IG wrote, "Reassuring statements that the [intelligence community] is currently using AI technologies - and will use AI technologies in the future - in ways consistent with the rule of law and American values will not be sufficient. The [agencies] will need to validate those statements for the American people." "Investment asymmetry between mission performance and intelligence oversight in AI efforts could lead to an accountability deficit," the statement continues, "there is little indication that investments in oversight of AI are currently a high priority."

III. Other key developments

A. President Issues Executive Order on Collecting Information About Citizenship Status

On June 28, 2019, the Supreme Court held that decision of Secretary of Commerce Ross to add a citizenship question to the Census 2020 was not supported by the evidence and that the rationale provided – to ensure enforcement of the Voting Rights Act – was "contrived."[97] The practical consequence of the decision was to prevent the question about citizenship from appearing on the 2020

---

[91] *Id*.
[92] *Id*.
[93] Letter from EPIC to Dep't of Defense (Feb. 22, 2019), https://epic.org/foia/dod/EPIC-19-02-22-DOD-FOIA-20190222-Request.pdf.
[94] *Id*.
[95] Kelsey Atherton, *Why won't the National Security Commission share its thoughts on AI?*, C4ISRNET (July 15, 2019), https://www.c4isrnet.com/artificial-intelligence/2019/07/15/national-security-commission-on-ai-meets-again/.
[96] Office of the Inspector Gen. of the Intelligence Community, Semiannual Report October 2018 - March 2019 (2019), https://www.dni.gov/files/ICIG/Documents/Publications/Semiannual%20Report/2019/ICIG%20Semiannual%20Report%20-%20October%202018%20to%20March%202019.pdf.
[97] *Dep't of Commerce v. New York*, 139 S.Ct. 2551, 2575 (June 27, 2019).

census. Following the decision, President Trump announced an Executive Order concerning "Collecting Information about Citizenship Status in Connection with the Decennial Census."[98]

In the Executive Order, the President stated that he is "ordering all agencies to share information requested by the Department [of Commerce] to the maximum extent permissible under law."[99] The President further stated that he is establishing "an interagency working group with a goal of making available to the Department administrative records *showing citizenship data for 100 percent of the population*."[100] The document "order[s] the Secretary of Commerce to consider mechanisms for ensuring that the Department's existing data-gathering efforts expand the collection of citizenship data in the future."[101] And it states that the President is "directing the Department to strengthen its efforts, consistent with law, to obtain State administrative records concerning citizenship."[102]

The President set out several arguments to ensure that "the Department has available the best data on citizenship that administrative records can provide, consistent with law, . . ."[103] Among those interests noted in the document is the identification of those who are eligible for public benefits. The Executive Order also concludes "data identifying citizens will help the Federal Government generate a more reliable count of the unauthorized alien population in the country."

The Executive Order states, "generating accurate data concerning the total number of citizens, non-citizens, and illegal aliens in the country has nothing to do with enforcing immigration laws against particular individuals. It is important, instead, for making broad policy determinations. . . . Administration, the data confidentiality protections in Title 13 shall be fully respected." However, on the same day that the President issued the Executive Order, the New York Times reported that Immigration and Customs Enforcement would renew "[n]ationwide raids to arrest thousands of members of undocumented families." The Order is likely to be subject to court challenge.

B. FOIA Access to Government Records Limited by Supreme Court

In *Food Marketing Institute v. Argus Leader Media* the Supreme Court narrowed public access to government documents by expanding the definition of "confidential" information.[104] *Food Marketing Institute* challenged a federal court decision to require an agency to release data on low income food program. The question was whether an exemption to FOIA applied to require the government to withhold all confidential commercial information requested regardless of whether there would be substantial harm to the company from release.

---

[98] Executive Order on Collecting Information about Citizenship Status in Connection with the Decennial Census (July 11, 2019), https://www.whitehouse.gov/presidential-actions/executive-order-collecting-information-citizenship-status-connection-decennial-census/.
[99] *Id.*
[100] *Id*. (emphasis added).
[101] *Id*.
[102] *Id*.
[103] *Id*.
[104] EPIC, *Food Marketing Institute v. Argus Leader Media*, Epic.org, https://epic.org/amicus/foia/food-marketing/.

The 6-3 decision by Justice Gorsuch overturned four decades of caselaw which held that a company must show substantial competitive harm to block an open government request. Writing in dissent, Justice Breyer, joined by Justices Ginsburg and Sotomayor, emphasized that the FOIA required some showing of harm to prevent public release of business records collected by federal agencies. "The whole point of FOIA is to give the public access to information it cannot otherwise obtain."

EPIC filed an amicus brief in the case warning the Court that removing the harm requirement "would deprive the public, and government watchdogs such as EPIC, of access to important information about 'what the government is up to'"[105] EPIC described several of its own FOIA cases, such as the case concerning airport body scanners, where access to commercial records made possible meaningful oversight and reform.[106] EPIC also warned that private parties, "acting on behalf of public agencies and with public funding," often hide their activities. EPIC wrote, "The public must have access to commercial information in agency records to conduct effective oversight of government programs that implicate privacy."

C. State Department to Require Social Media IDs of Visa Applicants

The State Department has now began to require all visa applicants submit social media identifiers to the federal government, after proposing the plan in March 2018.[107] EPIC long opposed the agency's plan, warning that "this proposal leaves the door open for abuse, mission creep, and the disproportionate targeting of Muslim and Arab Americans."[108] EPIC urged the agency to retract the proposal, pointing out the substantial privacy, free expression, and security concerns the proposal raised.[109] Last year, EPIC and the Brennan Center led a coalition of 55 privacy, civil liberties, and civil rights organizations in opposition to the State Department plan.[110]

---

[105] Brief of Amici Curiae Electronic Privacy Information Center (EPIC) and Twenty Legal Scholars and Technical Experts in Support of Respondent, Food Mktg. Inst. V. Argus Leader Media D/B/A Argus Leader, No. 18-481 (Mar. 25, 2019), https://epic.org/amicus/foia/food-marketing/Food-Marketing-v-Argus-SCOTUS-EPIC-Amicus.pdf

[106] EPIC, *EPIC v. FTC (Facebook Assessments)*, Epic.org, https://epic.org/foia/ftc/facebook/.

[107] Public Notice 10261, 83 Fed. Reg. 13806 (Mar. 30, 2018), https://www.gpo.gov/fdsys/pkg/FR-2018-03-30/pdf/2018-06490.pdf

[108] Comments of EPIC to the Dep't of State on Supplemental Questions for Visa Applicants (Dec. 27, 2017), https://epic.org/EPIC-DOS-Visas-SocialMediaID-Dec2017.pdf.

[109] Comments of EPIC to the Dep't of State on Proposed Information Collection for Visa Applicants (Sept.. 27, 2018), https://epic.org/apa/comments/EPIC-Comments-DOS-Social-Meida-IDs-Sept2018.pdf.

[110] Comments of EPIC, et al., to Dep't of State on Proposed Information Collection for Visa Applicants (May 29, 2018), https://epic.org/privacy/Coalition-Comments-DOS-Visa-Social-Media-Collection-May2018.pdf.

D. FAA Proposals Fall Short on U.S. Drone Privacy Rules

While the EU recently adopted a drone regulation require the real-time broadcasting of certain data, the FAA has yet to adopt comprehensive privacy rules for drone use in the U.S.[111] The Federal Aviation Administration recently published an interim final rule that will require a visible registration number on the exterior of drones. Previously, registration numbers could be hidden inside drones. While external markings are preferable to hidden identifiers, the rule did not go far enough.[112] In comments to the FAA, EPIC wrote, "Because drones present substantial privacy and safety risks, EPIC recommends that the FAA require any drone operating in the national airspace system to broadcast location when aloft (latitude, longitude, and altitude), course, speed over ground, as well as owner identifying information and contact information[.]"[113]

EPIC has repeatedly urged the FAA to adopt comprehensive rules for drones and specifically to ensure that drones broadcast in real-time location and identifying information.[114] "Because drones present substantial privacy and safety risks" EPIC has recommended "that the FAA require any drone operating in the national airspace system to broadcast location when aloft (latitude, longitude, and altitude), course, speed over ground, as well as owner identifying information and contact information."[115] EPIC recently wrote to the FAA noting the failure to keep pace with privacy developments and urging that the FAA include experts in privacy and security in its Drone Advisory Committee.[116] Senators Edward Markey (D-MA) and John Thune (R-SD) also recently wrote to the agency, urging the quickly publication of a rule for the real-time, remote identification of drones to "enhance safety, security, and privacy."[117]

EPIC also obtained records from the FAA's Drone Advisory Committee confirming the committee ignored the privacy risks posed by the deployment of drones—even after

---

[111] Commission Regulation 2019/945, 2019 O.J. (L 152) 1.
[112] External Marking Requirement for Small Unmanned Aircraft, 84 Fed. Reg. 3669-3673 (Feb. 13, 2019), https://www.federalregister.gov/documents/2019/02/13/2019-00765/external-marking-requirement-for-smallunmanned-aircraft.
[113] Comments of EPIC, et al., to the FAA on External Marking Requirement for Small Unmanned Aircraft (Mar. 15, 2019), https://epic.org/apa/comments/EPIC-Coalition-Comments-FAA-DroneID-Mar2019.pdf.
[114] Comment of EPIC to the FAA on Operation of Small Unmanned Aircraft Systems Over People (Apr. 15, 2019), https://epic.org/apa/comments/EPIC-Comments-FAA-Drones-Over-Ppl-Apr-2019.pdf; Comment of EPIC to the FAA on Safe and Secure Operations of Small Unmanned Aircraft Systems (Apr. 15, 2018), https://epic.org/apa/comments/EPIC-Comments-FAA-Drone-Security-Apr2019.pdf
[115] Comments of EPIC, et al., to the FAA, External Marking Requirement for Small Unmanned Aircraft (Mar. 15, 2019), https://epic.org/apa/comments/EPIC-Coalition-Comments-FAA-DroneID-Mar2019.pdf.
[116] Letter from EPIC to the FAA (July 1, 2019), https://epic.org/privacy/drones/EPIC-FAA-DAC-July2019.pdf.
[117] Letter from Sen. Markey & Sen. Thune to the FAA (Apr. 29, 2019), https://www.markey.senate.gov/imo/media/doc/Remote%20Indentification.pdf.

identifying privacy as a top public concern.[118] EPIC filed suit last year to enforce the transparency obligations of the industry-dominated Committee, which conducted much of its work in secret.[119] The documents show that the Committee initially recognized the importance of regulating drone privacy risks and even planned to form a "Privacy Subcommittee."[120] Yet the Committee entirely failed to address privacy issues before making final policy recommendations to the FAA.

The failure of the FAA to establish privacy safeguards for drones stands in sharp contrast to the decision of the European Commission earlier this year to adopt a comprehensive regulation for drones for the EU.[121]

E. Department of Homeland Security Face Recognition Expansion

The Department of Homeland Security (DHS) is expanding the use of facial recognition technology to domestic and international travelers and to conduct law enforcement.[122] The programs create serious risks to privacy and civil liberties, have been implemented without proper safeguards in place or explicit Congressional approval, and will impact millions of individuals, both U.S. and non-U.S. persons.

The most significant use of face recognition technology is the Customs and Border Protection's (CBP) Biometric Entry-Exit program. The program CBP uses facial recognition for all travelers entering and exiting the United States. CBP has rolled out the program without opportunity for public comment or specific legal authority. While the agency uses its own equipment as well as that of private firms, other government agencies, and foreign governments to capture face images,[123] but "no formal rules restricting the use of the photos captured by non-CBP owned equipment."[124]

EPIC and a coalition of civil society organizations called for Congress to suspend DHS's use of facial recognition. The letter cites extensive legal and practical shortfalls of the Entry-Exit Program:

---

[118] EPIC, *EPIC v. DAC: Records Show FAA Drone Committee Ignored Privacy Risks*, Epic.org (May 31, 2019), https://epic.org/2019/05/epic-v-dac-records-show-faa-dr.html.
[119] EPIC, *EPIC v. Drone Advisory Committee*, Epic.org, https://epic.org/privacy/litigation/faca/epic-v-drone-advisory-committe/.
[120] Drone Advisory Committee Survey (2016), https://epic.org/privacy/litigation/faca/epic-v-drone-advisory-committe/Drone-Advisory-Committee-survey-sept-2016.pdf (obtained by FOIA).; Drone Advisory Committee (DAC)—Task Group 1 Recommended Tasking on Roles and Responsibilities (2016) https://www.epic.org/privacy/litigation/faca/epic-v-drone-advisory-committe/EPIC-v-Drone-AdvisoryCommission-DAC-Survey-Sept-2016.pdf (obtained by FOIA).
[121] Commission Regulation 2019/945, 2019 O.J. (L 152) 1.
[122] Letter from EPIC, et al., to Comm. on Homeland Security (July 9, 2019), https://epic.org/privacy/facerecognition/HSC-Letter-DHS-Suspension-FRT.pdf.
[123] U.S. Dep't of Homeland Sec., U.S. Customs and Border Protection, DHS/CBP/PIA-0056, Privacy Impact Assessment for the Traveler Verification Service, 7-8 (Nov. 14, 2018) https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp030-tvs-november2018_2.pdf.
[124] Letter from EPIC, et al., to Comm. on Homeland Security, *supra* note 122.

> The Biometric Entry-Exit program is flawed. A report on iris and facial recognition technologies at a southern land border found that the technologies did not perform operational matching at a "satisfactory" level. A DHS Office of the Inspector General ("IG") report found that CBP's Biometric Entry-Exit program suffered from technical and operational challenges. … Travelers routinely report on burdensome procedures intended to compel individuals to undergo facial recognition even if that is not their choice.14 Additionally, CBP has not undergone formal rulemaking addressing how information collected will be used, disclosed, and retained, and what remedies will exist in cases where individuals are adversely impacted by the use of the technology. These concerns are further amplified given that CBP uses face recognition technology for purposes that extend far beyond simply verifying whether someone purportedly matches the photograph on their travel document.[125]

The privacy security risks of stockpiling sensitive personal data are also clear following a CBP subcontractor data breach in June 2019, exposing photographs and license plate readers of extraordinary breach of the images of travelers' faces and license plates.[126]

IV. Conclusion

EPIC welcomes close review of the EU-U.S. Privacy Shield by the European Commission. While we note that PCLOB is operational and that there is now a Privacy Ombudsman at the Department of Commerce, we also find that there has been no progress in modernizing U.S. privacy law, no establishment of a U.S. data protection agency, and no reform of Section 702 which permits bulk surveillance of the private communications of non-U.S. persons. Since the last review of the Privacy Shield, the U.S. has also pushed forward aggressive surveillance measures at the border, including facial recognition and the collection of social media identifiers.

We look forward to the Commission's final report.

Sincerely,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President

/s/ Eleni Kyriakides
Eleni Kyriakides
EPIC International Counsel

[125] *Id*.
[126] Drew Harwell, *Hacked documents reveal sensitive details of expanding border surveillance*, Wash. Post (June 21, 2019), https://www.washingtonpost.com/technology/2019/06/21/hacked-documents-reveal-sensitivedetails-expanding-border-surveillance/.