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

EUROPEAN COMMISSION
Privacy Shield Second Annual Review

August 14, 2018

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 second annual review of the EU- U.S. Privacy Shield.[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 the U.S. Congress,[3] participates in the U.S. administrative agency rulemaking process, [4] and litigates landmark privacy cases.[5]

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 frameworks.[7] EPIC has a long history of participation in the

---

[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
[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 2016), available at: https://epic.org/bookstore/.

debate over trans-Atlantic data flows. EPIC and a coalition of EU and U.S. consumer organizations 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."[8] EPIC President Marc Rotenberg outlined the shortcomings in Safe Harbor protection in testimony before the European Parliament[9] and U.S. Congress.[10] And, after serving as the sole U.S. NGO *amicus* in national court, EPIC is now 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.[11] EPIC has long made clear its support for comprehensive, meaningful, and effective legal protections for personal data.

We appreciate the opportunity to provide input into the European Commission's second annual review of the EU-U.S. Privacy Shield. The Commission requested information concerning U.S. law developments since October 2017 the are relevant to the Shield. Accordingly, Part I provides updates on U.S. surveillance and law enforcement access to personal data, and Part II updates on U.S. consumer privacy protection. Finally, Part III includes several other relevant news items on U.S. privacy protection.

I. National Security and Law Enforcement Access to Data

A. Carpenter v. United States *Decision Extends Fourth Amendment to Cell Phone Location*

In landmark ruling *Carpenter v. United States*, the Supreme Court held that the Fourth Amendment protects location records generated by mobile phones.[12] Law enforcement typically uses cell site location information ("CSLI") records in an investigation to pinpoint the location of individuals and create a map their movements over time. In *Carpenter*, the government obtained over five months of CSLI without a warrant based on probable cause, and used this data to create maps

[8] Letter from EPIC, et. al, to Isabelle Falque Pierrotin, Chairman, Article 29 Working Party, et. al (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/.
[9] 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.
[10] 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.
[11] EPIC, *Data Protection Commissioner v. Facebook & Max Schrems (CJEU)*, Epic.org, https://epic.org/privacy/intl/DPC-v-Facebook-CJEU/.
[12] *Carpenter v. United States*, 138 U.S. 2206, 2223 (2018).

showing that the plaintiff's cell phone had been near four of the charged robberies.[13] The Court declined to "to grant the state unrestricted access to a wireless carrier's database of physical location information," and concluded that the policy police must get a warrant when collecting at over seven days' worth of CSLI.[14]

In the decision by the Chief Justice John Roberts, the Court emphasized the importance of protecting privacy as technology advances: "As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to 'assure[ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'"[15] The Court held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through" a cell phone.[16] Dissenting opinions were filed by Justices Kennedy, Thomas, Alito, and Gorsuch.

Typical of Fourth Amendment caselaw, the *Carpenter* decision draws no distinction between the cell site information of U.S. persons and the cell cite information of non-US persons. As a consequence, a judicial warrant will be required when such information is sought in both instances. However, the Fourth Amendment rights of non-U.S. persons outside of the United States are still limited.[17]

EPIC, along with thirty-six technical *e*xperts and legal scholars, filed an amicus brief supporting the application of the warrant standard to obtain location data.[18] Since the ruling, EPIC has argued that Congress should update privacy law to address the challenges of other new technologies in use by law enforcement such as Stingrays - devices that can triangulate the source of a cellular signal and discretely collect vast troves of non-target, non-pertinent data.[19]

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

On March 23, 2018, President Trump signed the Clarifying Lawful Overseas Use of Data (CLOUD) Act into law. The CLOUD Act provides trans-border access to communications data in

[13] *Id.* at 2212–13.
[14] *Id.*
[15] *Id.* at 2214.
[16] *Id.* at 2217.
[17] *See, e.g.*, *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990) (requiring non-U.S. person located abroad have substantial voluntary connections in order to garner Fourth Amendment protection).
[18] Brief for EPIC and Thirty-Six Technical Experts and Legal Scholars as Amici Curiae in Support of Petitioner, *Carpenter v. United States*, No. 16-402 (Aug. 14, 2017), https://epic.org/amicus/location/carpenter/Carpenter-v-US-amicus-EPIC.pdf.
[19] Letter from EPIC to Rep. Ralph Abraham, Chairman, H. Comm. on Science, Space, & Tech. and Rep. Don Beyer, Ranking Member (June 27, 2018), https://epic.org/testimony/congress/EPIC-HSC-Stingrays-June2018.pdf.

criminal law enforcement investigations.[20] The Act represents a paradigm shift in the system cross-border access to data in criminal investigations: it authorizes law enforcement in one jurisdiction to order production of data stored in third country, without a layer of judicial or other review in the third country. EPIC repeatedly raised concerns about the level of protection afforded by the CLOUD Act and the need to respect national and international legal requirements,[21] and significant concerns about Privacy Shield's validity post-CLOUD Act have already been cited in the July 5th European Parliament resolution.[22]

The CLOUD Act is composed of two key elements: it provides U.S. access to foreign stored data, and it allows U.S. officials to create executive agreements for foreign access to U.S. stored data. First, the Act amends U.S. law to authorize U.S. law enforcement to order service providers to produce data located outside the U.S.[23] The interests of the nation where the data is stored are not considered until and unless a challenge is brought against the order in court.[24] However, only companies, not individuals, have an opportunity to challenge such orders, leaving the defense of individual rights dependent on service providers.

Still further, the challenges permitted by companies to U.S. orders for foreign are strictly limited. A provider is permitted to challenge the order to produce communications content only if the communications concern a foreign person residing outside of the U.S. and the company's compliance would risk violating foreign law of a "qualifying foreign government."[25] To be a "qualifying foreign government" the foreign nation must both have an executive agreement (described below) with the U.S. and have laws that provide a similar opportunity for U.S. companies to challenge orders within its jurisdiction.[26] If the foreign country meets these criteria, a U.S. court will then consider the challenge to an order, including using a "comity" analysis to assess foreign interests at stake.[27] The court *is permitted* but not required to modify or quash the order if it finds the laws of the foreign government would be violated, based on the "totality of the circumstances… interests of justice dictate" modifying or quashing the order, and the individual is determined to be a foreign person residing outside of the U.S.[28]

---

[20] Consolidated Appropriations Act, 2018, H.R. 1625, Div. V, 115th Cong., 2d Sess. (2018) (including the CLOUD Act) [hereinafter CLOUD Act].
[21] Comments of EPIC to the Nat'l Telecomm. Info. Admin. on International Internet Policy Priorities 11-12 (July 31, 2018), https://epic.org/apa/comments/EPIC-NTIA-International-July2018.pdf.
[22] *See, e.g.*, Resolution on the Adequacy of the Protection Afforded by the EU-U.S. Privacy Shield, Eur. Parl. Doc. P8_TA-PROV(2018)0315 (2018), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+MOTION+B8-2018-0305+0+DOC+PDF+V0//EN.
[23] CLOUD Act § 103.
[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] *Id.*

Second the Act also authorizes U.S. federal officials to enter into executive agreements granting foreign access to data stored in the U.S.[29] After the U.S. Attorney General, with the concurrence of the Secretary of State, provides certain certifications to the U.S. Congress, the agreement takes effect after 180 days unless Congress formally object within that timeframe. Specifically, these U.S. officials must certify that foreign government's domestic law and implementation of that law both provide sufficient substantive and procedural protections for privacy and civil liberties and the foreign government has adopted appropriate procedures to minimize data concerning U.S. persons. Additionally, these officials must certify the executive agreement reached meets a number of additional criteria, including requiring the foreign government not to target U.S. persons, that orders be limited to addressing serious crime, list a specific identifier, comply with the foreign nation's domestic law, and be subject to independent review or oversight.[30]

EPIC has argued that these protections required of executive agreements under the CLOUD Act should be increased in any negotiated agreement to meet human rights criteria set out by European Court of Human Rights and European Court of Justice decisions.[31] For instance, while notice to the data subject is generally required by international law, the CLOUD Act does not mandate notice to the data subject be a requirement for orders issued by a foreign government under an executive order.[32] Additionally, both courts have recognized the importance of systems of post-authorization supervision.[33] EPIC urges, at a minimum, requirement for aggregate statistical reporting of the number and types of orders under executive agreements.

C. Section 702 Reauthorized Without Privacy Safeguards

On January 19, 2018 President Trump signed the FISA Amendment Reauthorization Act of 2018 into law, reauthorizing Section 702 of the Foreign Intelligence Surveillance Act (FISA).[34] 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 judicial review of individual surveillance orders.[35] The FISA Amendment Reauthorization Act of 2018 renews Section 702 of the Foreign Intelligence Surveillance

---

[29] CLOUD Act § 105.
[30] *Id.*
[31] *See, e.g.*, Comments from EPIC to the United Nations Office of the High Comm'r on Human on "the right to privacy in the digital age" (Apr. 6, 2018), https://epic.org/privacy/intl/Comments-OHCHR-Digital-Age.pdf
[32] 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.
[33] *Id.*
[34] The FISA Amendment Reauthorization Act of 2018, Public Law No: 115-118, 132 Stat. 3 (2018).
[35] EPIC, *Foreign Intelligence Surveillance Act (FISA)*, Epic.org https://epic.org/privacy/surveillance/fisa/.

Act for six years. The reauthorization legislation raises two key issues for EU-U.S. Privacy Shield review: the Act's failure to extend any privacy protections to non-U.S. persons, and the Act's express authorization to restart "about" collection.

First, the FISA Amendments Reauthorization Act failed to 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, culminating in the landmark 2015 European Court of Justice *Schrems* decision overturning the Safe Harbor agreement.[36] Without a revision of U.S. surveillance practices, the U.S. legal regime vulnerable same criticisms lodged by the CJEU in 2015 of national security authorities' "access [to data] on a generalized basis." Nonetheless, extending any new privacy protections to non-U.S. persons - such as writing Presidential Policy Directive 28 which extends certain protections to non-U.S. persons, into law - were never meaningfully considered during the legislative debate over 702's reauthorization.

Second, the FISA Amendments Reauthorization Act expressly authorized U.S. intelligence agencies to restart "about" collection, reversing a change heralded by European bodies like the Article 29 Working Party.[37] 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."[38] In conducting "about" collection, government access to communications is broader than other means of collection; 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.[39] The NSA ended the program in 2017 because it was unable to comply with privacy strictures put in place by the FISC.[40] However, the Act permits the government to restart this controversial "about" collection program after providing thirty-days' notice to Congress.[41]

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

The 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 intelligence oversight reports. The PCLOB, established by the recommendation of the 9/11 Commission, provides oversight

---

[36] C-362/14, *Schrems v. Data Prot. Comm'r*, 2015 E.C.R. 650.
[37] *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.
[38] 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]
[39] *Id.*
[40] 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.
[41] FISA Amendment Reauthorization Act § 2.

and advice over U.S. intelligence activities.[42] However, it currently has no Chair and has had only one out of its four board members since January 2017.[43] Without a quorum, the PCLOB cannot initiate new activities nor provide advice in an official capacity.[44]

The PCLOB reports on FISA Sections 215 and 702 in the aftermath represented pivotal moment for U.S. intelligence transparency and reform.[45] For instance, these reports helped spur passage of the first major U.S. surveillance reform measure, the USA Freedom Act.[46] 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 PPD-28.[47] 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.[48]

After a long delay, there are now five nominees to the PCLOB. Adam Klein, a senior fellow at national security and defense think tank Center for New American Security, was nominated in Summer 2017.[49] Klein has expressed the view that the privacy intrusion of certain Section 702 practices is limited.[50] 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."[51] More recently, in March 2018 Ed Felten and Jane Nitze were nominated to join the Board.[52] 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. All three

---

[42] *History and Mission*, PCLOB.gov, https://www.pclob.gov/about/.
[43] *Id.*
[44] *Id.*
[45] *See* Privacy and Civil Liberties Oversight Bd., Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court (2014); PCLOB 702 Report, *supra* note 38.
[46] USA FREEDOM Act, Pub. L. No. 114-23, 129 Stat. 268 (2015).
[47] Privacy & Civil Liberties Oversight Bd., Semi-Annual Report: October 2015-March 2016 (2016), https://www.pclob.gov/library/Semi_Annual_Report_August_2016.pdf
[48] *See, e.g.*, Resolution on the Adequacy of the Protection Afforded by the EU-U.S. Privacy Shield, *supra* note 22.
[49] *Hearing on the Nomination of Adam Klein*, 115th Cong. (2018), https://www.judiciary.senate.gov/meetings/01/24/2018/nominations.
[50] 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.
[51] Letter from EPIC to Sen. Chick Grassley, Chairman, S. Comm. on the Judiciary, and Richard Blumenthal, Ranking Member (Jan. 23, 2018), https://epic.org/EPIC-SJC-PCLOB- Jan2018.pdf.
[52] 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/.

nominees have been approved by the Senate Judiciary Committee but have yet to receive a hearing or vote before the full Senate - the final step necessary to finalize their appointments.[53]Two nominees were recently announced: Travis LeBlanc - a partner at law firm Boies Schiller Flexner, an appointed arbitrator of the Privacy Shield, and former Federal Communications Commission Enforcement Bureau Chief widely recognized as a strong candidate - and Aditya Bamzai - an associate law professor at the University of Virginia and former Department of Justice attorney.[54]

E. Privacy Shield Ombudsperson Still Un-Appointed

The U.S. has failed to appoint a Privacy Shield Ombudsperson to receive complaints concerning U.S. surveillance, a clear requirement of the EU-U.S. Privacy Shield.[55] A holdover official from the Obama administration still temporarily holds the position - Principle Deputy Assistant Secretary for the Bureau of Oceans and International Environmental and Scientific Affairs Judy Garber.[56] As recently as August 1, 2018, a spokeswoman told the U.S. press that that the State Department has "no updates at this time" on the appointment of an Ombudsperson[57] EPIC recently wrote to the U.S. Congress indicating the urgency of a Privacy Shield Ombudsperson appointment.[58]

II. Consumer Privacy Protection

A. FTC Chronically Fails to Enforce Legal Judgments

While 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. FTC privacy enforcement depends primarily upon the agency's willingness to enforce the legal judgments (Consent Orders) it obtains against companies for deceptive or unfair corporate practices under Section 5 of the FTC Act.[59] Enforcement of Privacy

---

[53] Cristiano Lima, *Facebook gets out in front of the storm*, Politico Morning Tech (Aug. 1, 2018), https://www.politico.com/newsletters/morning-tech/2018/08/01/facebook-gets-out-in-front-of-the-storm-302902.

[54] White House, *President Donald J. Trump Announces Intent to Nominate Personnel to Key Administration Posts*, Whitehouse.gov (Aug. 7, 2018), https://www.whitehouse.gov/presidential-actions/president-donald-j-trump-announces-intent-nominate-personnel-key-administration-posts-57/.

[55] *See, e.g.*, Resolution on the Adequacy of the Protection Afforded by the EU-U.S. Privacy Shield, *supra* note 22.

[56] *Privacy Shield Ombudsperson*, State.gov, https://www.state.gov/e/privacyshield/ombud/.

[57] Cristiano Lima, *supra* note 54.

[58] Letter from EPIC to John Culberson, Chairman House Comm. on Appropriations, Jose Serrano, Ranking Member (Mar. 20, 2018), https://epic.org/testimony/congress/EPIC-HAC- Commerce-Mar2018.pdf.

[59] Codified at 15 U.S.C. Sec. 45(a)(1) ('Unfair methods of competition in or affecting commerce ... are hereby declared unlawful.').

Shield expressly relies on the FTC's effective use of Section 5 authority.[60] However, when the FTC does reach a consent agreement with a privacy-violating company, the Commission routinely fails to enforce it.[61] The most recent effect of this failure is the unlawful disclosure of 50 million Facebook user records to controversial data mining firm Cambridge Analytica.[62]

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.[63] The unlawful disclosure of user records to the data mining firm likely violated a 2011 FTC Consent Order against Facebook, an order which was the result from a sustained campaign by US privacy organizations.[64] 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 users.[65] In 2011, the FTC agreed with EPIC and established a far-reaching settlement with the company that prevented such disclosures, prohibited deceptive statements, established independent auditing, and required annual reporting over 20 years.[66]

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."[67]

---

[60] FTC, *Privacy Shield*, FTC.gov, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/privacy-shield.
[61] *See EPIC v. FTC*, No. 12-206 (D.C. Cir. Feb. 8, 2012).
[62] Letter from EPIC, et. al, to Maureen Ohlhausen, Acting Chairman, Fed. Trade Comm'n, and Terrell McSweeney, Comm'r (Mar. 20, 2018), https://epic.org/privacy/facebook/EPIC-et-al-ltr-FTC-Cambridge-FB-03-20-18.pdf.
[63] 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.
[64] Marc Rotenberg, *How the FTC Could Have Prevented the Facebook Mess*, (Mar. 22, 2018), https://techonomy.com/2018/03/how-the-ftc-could-have-avoided-the-facebook-mess/; Letter from EPIC to Maureen Ohlhausen, Acting Chairman, Fed. Trade Comm'n (Feb. 15, 2017), https://epic.org/privacy/internet/ftc/EPIC-et-al-ltr-FTC-02-15- 2017.pdf.
[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] 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.
[67] Letter from EPIC, *et. al,* to Maureen Ohlhausen, Acting Chairman, Fed. Trade Comm'n, and Terrell McSweeney, Comm'r (Mar. 20, 2-018), https://epic.org/privacy/facebook/EPIC-et-al-ltr-FTC-Cambridge-FB-03-20-18.pdf.

The FTC confirmed it has an open investigation into Facebook in March 2018.[68] At the time, Tom Pahl, Acting Director of the Federal Trade Commission's Bureau of Consumer Protection stated:

> The FTC is firmly and fully committed to using all of its tools to protect the privacy of consumers. Foremost among these tools is enforcement action against companies that fail to honor their privacy promises, including to comply with Privacy Shield, or that engage in unfair acts that cause substantial injury to consumers in violation of the FTC Act. Companies who have settled previous FTC actions must also comply with FTC order provisions imposing privacy and data security requirements.[69]

On July 5, 2018 the European Parliament passed a resolution calling for suspension of the Privacy Shield if the U.S. does not comply in full by September 1, 2017.[70] This resolution notes that Facebook and Cambridge Analytica (as well as parent company SCL Elections) are certified to collect the data of Europeans under the Privacy Shield.[71]

However, nearly five months have now passed since the new Commission announced it was reopening its investigation of Facebook,[72] and the FTC has still not issued a judgment or even a report. Over this time, the United States Congress has held three hearings on the matter, the European Parliament has held three hearings, and the UK ICO has conducted an extensive investigation, published a comprehensive report, and issued a substantial fine.[73]

---

[68] 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.

[69] *Id.*

[70] Resolution on the Adequacy of the Protection Afforded by the EU-U.S. Privacy Shield, *supra* note 22.

[71] *Id.*

[72] Press release, Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practices, *supra* note 69.

[73] *See* Facebook, Social Media Privacy, and the Use and Abuse of Data: Hearing Before the S. Comm. on the Judiciary, 115th Cong. (2018), https://www.judiciary.senate.gov/meetings/facebook-social-mediaprivacy-and-the-use-and-abuse-of-data (April 10, 2018); Press release, Third Facebook-Cambridge Analytica hearing: data breach prevention and cures (July 3, 3018), http://www.europarl.europa.eu/news/en/press-room/20180702IPR07037/third-facebook-cambridge-analytica-hearing-data-breach-prevention-and-cures; Information Commissioner's Office, *Investigation Into the Use of Data Analytics In Political Campaigns*, (Jul. 10, 2018), https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for- political-purposes-update.pdf.

B. Social Science One Access to Facebook User Data

EPIC has argued the FTC also subsequently failed to enforce the Consent Order against Facebook. One alarming example concerns a study by "Social Science One," a venture of US organizations with close ties to Facebook, to obtain the personal data of Facebook users from Facebook to pursue a wide range of initiatives, including the effect of social media on democracy and elections.[74] However, the 2011 Consent Order requires Facebook to obtain affirmative express consent before disclosing personal data to third parties.[75] By transferring personal information to third-party researchers without (1) providing clear and prominent notice and (2) obtaining the affirmative express consent of users, EPIC contends that Facebook will again violate the 2011 Consent Order with the FTC, the GDPR, and ethical obligations to obtain informed consent. EPIC wrote to the FTC and the European Data Protection Board, as well as to Social Science One calling for suspension of the transfer of user data.[76]

C. Full Slate of FTC Commissioners Nominated

In April 2018 the U.S. Senate confirmed five nominees to serve as Commissioners for the Federal Trade Commission. After a long delay, the FTC is back to full capacity after the FTC's leadership was reduced to only two Commissioners for 2017.[77] Antitrust attorney Joseph Simons, a Republican, will serve as chair of the Commission.[78] Senate staffer Noah Phillips and Delta Airlines vice president Christine Wilson will fill two Republican seats.[79] Former assistant director to the

---

[74] Social Science One, Independent Research Commission Partnering with Facebook and 7 Nonprofit Foundations to Study Role of Social Media in Elections and Democracy Reveals New Name and Announces First Data Set is Available for Academic Research (July 11, 2018), https://socialscience.one/blog/socialscience-one-public-launch.

[75] Fed. Trade Comm'n., In re Facebook, Decision and Order, FTC File No. 092 3184 (Jul. 27, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf; Fed. Trade Comm'n, Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises, Press Release (Nov. 29, 2011), https://www.ftc.gov/news-events/pressreleases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

[76] *See* Letter from EPIC to Joseph J. Simons, Chairman, Fed. Trade Comm'n, et. al (July 13, 2018), https://epic.org/privacy/facebook/EPIC-Letter-FTC-SocialScienceOne-July2018.pdf; Letter from EPIC to Professor Gary King, Co-chair, Social Science One, and Professor Nathaniel Persily, Co-chair, Social Science One (July 12, 2018), https://epic.org/privacy/facebook/EPIC-ltr-SocialScienceOne-July-2018.pdf.

[77] 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.

[78] Harper Neidig, *Trump nominates four potential FTC commissioners,* Hill (Jan. 25, 2018), http://thehill.com/policy/technology/370783-trump-nominates-full-slate-of-ftc-commissioners.

[79] *Id.*

Consumer Financial Protection Bureau Rohit Chopra will fill a Democratic seat.[80] Rebecca Kelly Slaughter, a second Senate staffer, joined the Commission will fill a second Democratic seat.[81] Commissioner Phillips is expected to take on the international portfolio.

Chairman Simons has announced that he plans to undertake an extensive inquiry on data protection and competition.[82] The FTC will examine "whether broad-based changes in the economy, evolving business practices, new technologies, or international developments might require adjustments to competition and consumer protection enforcement law, enforcement priorities, and policy."[83] According to the Commission, "The hearings may identify areas for enforcement and policy guidance, including improvements to the agency's investigation and law enforcement processes, as well as areas that warrant additional study."[84] The FTC is specifically exploring the "The intersection between privacy, big data, and competition" (topic 4). The FTC is requesting public comment in advance of the hearings. This will be the first time the FTC has reexamined its approach to consumer protection and competition since similar hearings held in 1995.[85]

EPIC fully supports this undertaking and will submit extensive comments. EPIC has also explained that enforcement must remain a priority. EPIC detailed how the FTC can accomplish its mission of protecting consumers and promoting competition in the 21st century, including fully enforcing its legal judgments and introducing legislative proposals to safeguard consumer privacy in comments on the FTC's Five Year Strategic Plan.[86]

---

[80] *Id.*

[81] Phillips, Slaughter, and Chopra Sworn in as FTC Commissioners (May 2, 2018), https://www.ftc.gov/news-events/press-releases/2018/05/phillips-slaughter-chopra-sworn-ftc-commissioners.

[82] Press release, FTC Announces Hearings On Competition and Consumer Protection in the 21st Century (June 20, 2018), https://www.ftc.gov/news-events/press-releases/2018/06/ftc-announces-hearings-competition-consumer-protection-21st?utm_source=govdelivery.

[83] Fed. Trade Comm'n., *Hearings On Competition and Consumer Protection in the 21st Century*, File No. P181201, 83 Fed. Reg. 3807, (Aug. 6, 2018), https://www.ftc.gov/system/files/documents/federal_register_notices/2018/07/p181201_fr_notice_announcing_competition_and_consumer_protection_hearings.pdf; *see also*, Fed. Trade Comm'n., *FTC Announces Hearings On Competition and Consumer Protection in the 21st Century*, Press Release (Jun. 20, 2018), https://www.ftc.gov/news-events/press-releases/2018/06/ftc-announces-hearings-competition-consumer-protection-21st.

[84] *Id.*

[85] Press release, Federal Trade Commission Hearings on Global and Innovation-Based Competition (Oct. 6, 1995), https://www.ftc.gov/news-events/press-releases/1995/10/federal-trade-commission-hearings-global-innovation-based.

[86] Comments of EPIC to Fed. Trade Comm'n 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.

D. U.S. Consumer Privacy Law: No Comprehensive Federal Law, While California Passes Strongest Consumer Privacy Law in the U.S.

Despite record-breaking data breaches, the U.S still lacks comprehensive privacy legislation. In fact, Congress has failed to enact any legislative proposal for consumer privacy since adoption of Privacy Shield.[87] On the other hand, California recently passed a landmark privacy law, though it does not go into force until 2020 and there is speculation that it will be weakened.

2017 marked the highest number of data breaches yet in the U.S., representing a grave lack of data security by U.S. companies.[88] The number of data breaches nearly doubled from 2016 to 2017.[89] Identity fraud increased by 16 percent in 2016, with a total of $16 billion stolen from 15.4 million U.S. consumers.[90] 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. The U.S. continues to operate without comprehensive privacy legislation, relying instead on a patchwork of sectoral laws.

On the other hand, there has been some notable progress on enhancing consumer privacy at the state level. The State of California has enacted the California Consumer Privacy Act of 2018, one of the most comprehensive state consumer privacy laws in the United States.[91] The Act establishes the right of residents of California to know what personal information about them is being collected; to know whether their information is sold or disclosed and to whom; to limit the sale of personal information to others; to access their information held by others; and to obtain equal service and price, even if they exercise their privacy rights.[92] The Act allows individuals to delete their data and it will establish opt-in consent for those under 16.[93] Finally, the Act also provides for enforcement by the

---

[87] Testimony and Statement of Marc Rotenberg, EPIC President, Hearing on Examining the Current Data Security and Breach Notification Regulatory Regime before the H. Comm on Banking, Housing, & Urban Affairs (Feb 14, 2018), https://epic.org/testimony/congress/EPIC-Testimony-HFS-2-14-18.pdf.

[88] *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

[89] *Id.*

[90] 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-usvictims-2016-16- percent-according-new.

[91] California Consumer Privacy Act of 2018 ("CCPA"), Cal. Civ. Code § 1798.198(a) (2018), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

[92] CCPA § 3.

[93] *Id.*

Attorney General, a private right of action, and establishes a Consumer Privacy Fund to support the purposes of Act.[94]

EPIC has long favored the establishment of a comprehensive privacy law in the United States.[95] The current mix of sectoral regulation and self-regulation is ineffective, inefficient, cumbersome, and costly, and the FTC lacks the ability, authority and expertise to engage today's broad range of challenges – Internet of Things, AI, connected vehicles, and more.[96] After the Equifax data breach, among the largest in U.S. history, EPIC testified in the U.S. Senate that comprehensive privacy legislation was long overdue.[97]

E. U.S. Still Without Data Protection Agency

The data breach epidemic, as detailed above, has reached unprecedented levels and the need for an effective, independent data protection agency has never been greater. Virtually every other advanced economy recognized the need for an independent agency to address the challenges of the digital age.[98] However, the U.S. still lacks a central data protection agency, hampering its ability to respond to today's vast challenges for data protection. Compounding the problem, federal agencies with jurisdiction over narrow aspects of privacy protection also often lack sufficient lack sufficient authority and resources. As a result, the current approach to privacy oversight and enforcement is unnecessarily inefficient, complex, and ineffective.[99]

The FTC is not a data protection agency. The FTC 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.[100] Relying on the FTC's current framework to address all consumer privacy concerns is not in the best interest of consumers. The Consumer Financial Protection Bureau (CFPB) similarly lacks data protection

---

[94] *Id.*
[95] *See, e.g.*, 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.
[96] *See* Comments of EPIC to the Nat'l Telecomm. Info. Admin. on Int'l Internet Policy Priorities, *supra* note 21 at 2.
[97] 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 , *supra* note 96.
[98] *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.
[99] *Id*
[100] 15 U.S.C. Sec. 45(a)(1).

authority and only has jurisdiction over financial institutions.[101] Neither agency possesses the expertise and resources needed to address data security across the country. The PCLOB, an independent agency with privacy oversight and advisory authority in the national security domain, lies dormant.[102] In contrast, an independent agency dedicated to data protection could more effectively utilize its resources to police the current widespread exploitation of consumers' personal information. An independent agency would also be staffed with personnel who possess the requisite expertise to regulate the field of data security.

EPIC has testified before Congress numerous times on the need for the U.S. to establish a data protection agency,[103] in addition to submitting letters to Congressional hearings[104] and comments to federal agencies urging the same.[105] However, the U.S. has failed to take steps toward forming a central agency.

III. Other key developments

A. *Judge Brett M. Kavanaugh Nomination to the U.S. Supreme Court Raises Privacy Concerns*

Judge Brett M. Kavanaugh was nominated to be the next Justice on the U.S. Supreme Court.[106] Kavanaugh would fill the place left by Anthony Kennedy who announced his retirement at the end of the last term.[107] Since 2006, Judge Kavanaugh has served on the U.S. Court of Appeals

---

[101] CFPB, *Institutions subject to CFPB supervisory authority*, Consumerfinance.gov, https://www.consumerfinance.gov/policy-compliance/guidance/supervision-examinations/institutions/.
[102] *See supra* Section I(D).
[103] *See, e.g.*, *id.*; 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 , *supra* note 96.
[104] *See, e.g.*, Letter from EPIC to Sen. Roger Wicker, Chairman, and Sen. Brian Schatz, Ranking Member, S. Comm, on Commerce Sci. & Transp, *supra* note 99.
[105] *See, e.g.*, Comments of EPIC to Fed. Trade Comm'n on Draft Strategic Plan for Fiscal Years 2018 to 2022, *supra* note 87.
[106] President Donald J. Trump Announces Intent to Nominate Judge Brett M. Kavanaugh to the Supreme Court of the United States (July 9, 2018), https://www.whitehouse.gov/presidential-actions/president-donald-j-trump-announces-intent-nominate-judge-brett-m-kavanaugh-supreme-court-united-states/.
[107] Robert Barnes, *Justice Kennedy, the Pivotal Swing Vote on the Supreme Court, Announces His Retirement*, Wash. Post (June 27, 2018), https://www.washingtonpost.com/politics/courts_law/justice-kennedy-the-pivotal-swing-vote-on-the-supreme-court-announces-retirement/2018/06/27/a40a8c64-5932-11e7-a204-ad706461fa4f_story.html.

for the District of Columbia.[108] Prior to his appointment to the Court, Judge Kavanaugh served as White House associate counsel and then staff secretary between 2001 and 2006.[109] During the period, the White House launched many programs of mass surveillance, including PNR, Total Information Awareness, the PATRIOT Act, and "Perfect Citizen."

The nomination of Kavanaugh to the Supreme Court has raised concerns about the future of privacy and Constitutional protections against government surveillance. As a judge on the D.C. Circuit Court of Appeals, Kavanaugh upheld the warrantless, widespread, and suspicionless collection of call records of Americans under Section 215 of FISA in *Klayman v. Obama*.[110] Kavanaugh authored a separate opinion in the case to state expressly that the mass surveillance program was lawful on two distinct grounds. First, writing pre-*Carpenter* Kavanuagh stated bulk metadata collection program "is entirely consistent with the Fourth Amendment" based on the third-party doctrine discussed above in Section I(A).[111] In a second claim, Kavanaugh stated that even if the search triggered constitutional concerns, it "fit comfortably" in the special needs exception to the Fourth Amendment.[112] "Critical national security need outweighs the impact on privacy occasioned by the program," Kavanaugh wrote.[113] Congress subsequently determined that the data collection activity that Kavanaugh endorsed was overly broad and terminated the program.[114] And even conservative legal scholars are skeptical of Kavanaugh's claim that the "special needs" doctrine permits warrantless surveillance without evidence in support of the special circumstances. [115]

There is widespread concern surrounding the secrecy of the Kavanaugh nomination.[116] In an unprecedented move coordinated with the National Archives, the Chairman of the Senate Judiciary Committee Senator Chuck Grassley has provided access to only a portion of the nominee's prior records.[117] Documents released by the Senate Judiciary Committee thus far show that Kavanaugh

---

[108] *Brett M. Kavanaugh*, D.C. Circuit, https://www.cadc.uscourts.gov/internet/home.nsf/Content/VL+-+Judges+-+BMK.
[109] *Id.*
[110] *Klayman v. Obama*, 805 F.3d 1148 (D.C. Cir. 2015) (Kavanaugh B. concurring), https://cases.justia.com/federal/appellate-courts/cadc/15-5307/15-5307-2015-11-20.pdf?ts=1448053378.
[111] 805 F.3d at 1149.
[112] *Id.*
[113] *Id.*
[114] USA FREEDOM Act, § 107
[115] Orin Kerr, *Judge Kavanaugh on the Fourth Amendment*, SCOTUSblog (July 20, 2018), http://www.scotusblog.com/2018/07/judge-kavanaugh-on-the-fourth-amendment/.
[116] Letter from EPIC, et. al, to George W. Bush (Aug. 8, 2018), https://www.openthegovernment.org/sites/default/files/Letter%20to%20President%20Bush%20re%20Kavanaugh.pdf.
[117] Letter from Sen. Dianne Feinstein, Ranking Member, S. Judiciary Comm., to David S. Ferriero, Archivist of the U.S., Nat'l Archives & Records Admin. (Aug. 6, 2018),

assisted in the effort to pass the Patriot Act and drafted a statement that President Bush incorporated in the bill signing. Kavanaugh wrote that the PATRIOT Act, a dramatic expansion of U.S. surveillance, would "update laws authorizing government surveillance," and, he continued in an email exchange, the Act was a "measured, careful, responsible, and constitutional approach."[118]

EPIC has submitted an urgent Freedom of Information Act Request for all records concerning Judge Kavanaugh's activity in the Bush Administration, to determine the extent of his involvement in the mass surveillance programs, including warrantless wiretapping, when he was in the White House.[119] EPIC also expects to ask Senate Judiciary Committee to question Kavanaugh on a wide range of privacy, First Amendment, open government, and consumer protection issues.[120]

B. White House Select Committee on Artificial Intelligence, Closed to Public, Sets U.S. Priorities

The White House has established the "Select Committee on Artificial Intelligence" to advise the President and coordinate AI policies among executive branch agencies.[121] The Office of Science and Technology Policy, NSF, and DARPA will lead the interagency committee.

According to its Charter, the Select Committee will address significant national and international policy matters that cut across agency boundaries, and will provide a formal mechanism for interagency policy coordination and the development of Federal artificial intelligence activities, including those related to autonomous systems, biometric identification, computer vision, human-computer interactions, machine learning, natural language processing, and robotics. [122] The Committee would also coordinate efforts across federal agencies to research and adopt new technologies.[123]

---

https://www.feinstein.senate.gov/public/_cache/files/3/a/3a647901-19cd-4e8a-9384-e57ef8a578b6/BDC417E3D6141BCB170B28CAB5423CC3.feinstein-to-archivist.pdf.

[118] Press release, Committee Releases First Production of Kavanaugh Records (Aug. 9, 2018), https://www.judiciary.senate.gov/press/rep/releases/committee-releases-first-production-of-kavanaugh-records.

[119] EPIC, *EPIC to Request Kavanaugh White House Records on Warrantless Wiretapping, Mass Surveillance Programs*, Epic.org (July 30, 2018), https://epic.org/2018/07/epic-to-request-kavanaugh-whit.html.

[120] EPIC has submitted similar statements to the Judiciary Committee for the hearings on past Justices, including the most recent nominee Justice Gorsuch. *See, e.g.*, EPIC, *Neil Gorsuch and Privacy*, Epic.org, https://epic.org/privacy/gorsuch/.

[121] White House Office of Science &Tech. Policy, Summary of the 2018 White House Summit on Artificial Intelligence for American Industry 7 (2018), https://www.whitehouse.gov/wp-content/uploads/2018/05/Summary-Report-of-White-House-AI-Summit.pdf.

[122] Charter of the National Science and Technology Council Select Committee on Artificial Intelligence (2018), https://epic.org/SelectCommitteeonAI.pdf.

[123] *Id.*

Despite the broad social implications of these topics, the Charter identifies only the "private sector" as a source of advice.[124]

However, the White House AI meeting and the first meeting of the Select Committee on AI were closed to the public. [125] Many of the critical issues in the AI field, including "fairness," "transparency," and "accountability," were never mentioned. [126] EPIC, leading scientific organizations, including AAAS, ACM and IEEE, and nearly 100 experts have petitioned the Office of Science and Technology Policy to solicit public comments on artificial intelligence policy.[127] EPIC has also submitted a Freedom of Information Act request for records about the establishment of the Select Committee.[128]

C. State Department Calls for Sweeping Social Media History of Visa Applicants

The U.S. State Department has issued a formal proposal to require immigrant and non-immigrant visa applicants to submit social media identifiers to the federal government.[129] Among other information, the State Department asks applicants to provide five years' worth of previously used social media identifiers, telephone numbers, email addresses, and travel history.[130] The proposal must be still approved by the Office of Management and Budget before taking effect.

EPIC, the Brennan Center and fifty-five privacy, civil liberties, and civil rights organizations submitted comments opposing the State Department's plan to collect social media identifiers from individuals applying for visas.[131] The coalition warned that the proposal would undermine rights of "speech, expression, and association," and "will reveal private information about travelers that is irrelevant to their suitability for entry to the United States, and will expose data about their families, friends and business associates in the U.S." [132] The policy will also "facilitate the bulk

---

[124] *Id.*
[125] Readout from the Inaugural Meeting of the Select Committee on Artificial Intelligence (June 27, 2018), https://epic.org/privacy/ai/WH-AI-Select-Committee-First-Meeting.pdf.
[126] White House Office of Science &Tech. Policy, *supra* note 124, at 7.
[127] Letter from EPIC, et. al, to Michael Kratsios, Deputy U.S. Chief Tech. Officer, Office of Science & Tech. Policy (July 4, 2018), https://epic.org/privacy/ai/OSTP-AI-Petition.pdf.
[128] Letter from Mario Trujillo, EPIC Clerk, and Enid Zhou, EPIC Open Government Fellow, to Bob Stafford, Acting Chief FOIA Officer, U.S. General Services Administration (June 25, 2018), https://epic.org/foia/gsa/EPIC-18-06-25-GSA-FOIA-20180625-Request.pdf.
[129] Public Notice 10261, 83 Fed. Reg. 13806 (Mar. 30, 2018), https://www.gpo.gov/fdsys/pkg/FR-2018-03-30/pdf/2018-06490.pdf.
[130] *Id.*
[131] Comments of EPIC, et. al, to Dep't of State on Supplemental Questions for Visa Applicants (May 29, 2018), https://epic.org/privacy/Coalition-Comments-DOS-Visa-Social-Media-Collection-May2018.pdf.
[132] *Id.* at 1-2.

mining and wide-ranging use of information about travelers," the coalition continued, all "in exchange for speculative national security benefits."[133]

D. Citizenship Question on US Census

The U.S. Census Bureau has announced the 2020 U.S. census will include a question on citizenship status.[134] The Census Bureau has not asked Americans about their citizenship status in almost 70 years.[135] Every ten years, as directed by the US Constitution the Government conducts a census of all individuals in the country.[136] The data is used for a variety of critical political and economic planning purposes in the United States. However, the Census also implicates numerous privacy issues, including the use of information to identify individuals rather than for the statistical collection of information.[137]

The addition of the citizenship question to the 2020 census has raised greater concerns about data confidentiality than previous decennial censuses. The Census Bureau conducted a study in 2017 that found respondents expressing new concerns including the "Muslim ban," the dissolution of DACA, and Immigration and Customs Enforcement.[138] The study found that these concerns were most pronounced among immigrant respondents.[139]

Such concerns reflect actual experience with the U.S census. Despite strong census privacy laws, the U.S. has a sordid history of misusing census data to target minority groups. The most egregious misuse of census data was the role it played in the internment of Japanese-Americans during World War II.[140] In 1943 the Census Bureau complied with a request by the Treasury Secretary for the

---

[133] *Id*. at 2.
[134] U.S. Census Bureau, *Proposed Information Collection; Comment Request; 2020 Census*, Notice, 83 FR 26643 (June 8, 2018), https://www.federalregister.gov/documents/2018/06/08/2018-12365/proposed-information-collection-comment-request-2020-census.
[135] *See* 1950 (Population) Census Questionnaire, Census Bureau, https://www.census.gov/history/www/through_the_decades/index_of_questions/1950_population.html (asking the question "If foreign born, is the person naturalized?").
[136] U.S. Const. art. II § 2, cl. 3.
[137] EPIC, T*he Census and Privacy*, EPIC.org, https://epic.org/privacy/census/.
[138] Center for Survey Measurement, MEMORANDUM FOR Associate Directorate for Research and Methodology (ADRM) Respondent Confidentiality Concerns (Sept. 20, 2017), https://www2.census.gov/cac/nac/meetings/2017-11/Memo-Regarding-Respondent-Confidentiality-Concerns.pdf.
[139] *Id.*
[140] JR Minkel, *Confirmed: The U.S. Census Bureau Gave Up Names of Japanese-Americans in WW II,* Scientific American (March 30, 2007), https://www.scientificamerican.com/article/confirmed-the- us-census-b/.

names and locations of all people of Japanese ancestry in the Washington, D.C., area.[141] In another example, after 9-11 EPIC pursued a Freedom of Information Act request about the potential misuse of census data. Documents obtained by EPIC revealed that the Census Bureau had provided the Department of Homeland Security ("DHS") with census data on individuals of Arab ancestry.[142] As a result of these revelations, resulting from EPIC's FOIA litigation, the Census Bureau revised its policy on sharing statistical information about "sensitive populations" with law enforcement or intelligence agencies.[143] Customs and Border Protection also changed its policy on requesting "information of a sensitive nature from the Census Bureau."[144]

The Bureau has also not given proper consideration to the privacy implications of collecting citizenship data. By law, federal agencies must create and publish a "Privacy Impact Assessment" (PIA) before personally identifiable information is collected, used, and maintained in federal systems.[145] PIAs assess the privacy risks of the collection and inform the public about the information collection. However, the PIA for the census contains no analysis of the new privacy risks raised by the new citizenship question.[146] The PIA is required to be updated "where a system change creates new privacy risks."[147]

In comments to the agency, EPIC specifically asks the Census Bureau to suspend the citizenship question from the 2020 census form until a PIA dealing specifically with the issues raised

---

[141] W. Seltzer and M. Anderson, "Census Confidentiality under the Second War Powers Act (1942-1947)." Paper prepared for presentation at the annual meeting of the Population Association of America, New York, March 29-31, 2007, *available at* http://studylib.net/doc/7742798/census-confidentiality-under-the-second-war-powers.

[142] *Department of Homeland Security Obtained Data on Arab Americans From Census Bureau*, EPIC, https://epic.org/privacy/census/foia/; Lynette Clemetson, *Homeland Security Given Data on Arab-Americans*, New York Times, Jul. 30, 2004, http://www.nytimes.com/2004/07/30/us/homeland-security-given-data-on-arab-americans.html.

[143] Census Bureau News, ''U.S. Census Bureau Announces Policy Regarding Sensitive Data,'' press release CB04-145, August 30, 2004; Lynette Clemetson, *Census Policy On Providing Sensitive Data Is Revised*, New York Times, Aug. 31, 2004, http://www.nytimes.com/2004/08/31/us/census-policy-on-providing-sensitive-data-is-revised.html.

[144] U.S. Customs and Border Protection, *Policy for Requesting Information of a Sensitive Nature from the Census Bureau*, Memorandum (Aug. 9, 2004), https://epic.org/privacy/census/foia/policy.pdf.

[145] E-Government Act of 2002, Pub. L. No. 107-347, § 208(b)(1)(A), 116 Stat. 2899 (2002).

[146] U.S. Department of Commerce, U.S. Census Bureau, *Privacy Impact Assessment for the CEN08 Decennial Information Technology Division* (July 28, 2018) http://www.osec.doc.gov/opog/privacy/Census%20PIAs/CEN08_PIA_SAOP_Approved.pdf.

[147] U.S. Department of Commerce, Office of Privacy and Open Government, *Privacy Compliance* http://www.osec.doc.gov/opog/privacy/compliance.html.

by the citizenship question is conducted.[148] In addition to citing concerns about discrimination and privacy, EPIC explained the new question subverts the agency's purpose and risks undermining data quality.[149]

IV. Conclusion

EPIC welcomes a close review of the EU-U.S. Privacy Shield by the European Commission. 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

/s/ Alan Butler
Alan Butler
EPIC Senior Counsel

[148] Comments of EPIC to Census Bureau on 2020 Census (Aug.7, 2018), Shttps://epic.org/privacy/Coalition-Comments-DOS-Visa-Social-Media-Collection-May2018.pdf.
[149] *Id.*