epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

International Working Group on Data Protection in Telecommunications
62nd Meeting
Paris, France, 27–28 November 2017

Country Report
United States of America
(provided by EPIC)

--

Table of Contents

--

I. Major U.S. Privacy Developments

Russian Interference with the 2016 Presidential Election

U.S. intelligence agencies and Congress have continued to evaluate the ongoing risk of Russian interference on U.S. election systems and develop a response for future attacks.

In a May, former Acting Attorney General Sally Yates said she warned the White House that General Michael Flynn "could be blackmailed by the Russians" who knew he had lied about his Russian contacts.[1] Yates also said the Department of Justice came forward out of concern that both administration officials and the American people "had been misled."[2] In June, a leaked National Security Agency document detailed Russian attempts to interfere in the 2016 Presidential Election via cyber-attacks.[3] The document concludes that the attacks were carried out by Russian military intelligence and involved spear-phishing emails and a cyber-attack on a private manufacturer of devices that maintained and verified the voter rolls.

Concern about Russian interference has led to several moves within Congress. Notably, in the proposed intelligence bill reauthorization for 2018, the Senate has included provisions reflecting widespread concern about the Russian interference in the 2016 Presidential Election.[4] Among other requirements, the bill mandates a report to Congress detailing the past cyber-attacks on election infrastructure and the risk of future attacks, as well as a report assessing the intelligence community response to the attacks.

In September, the Department of Homeland Security banned Russian security software maker, Kaspersky Lab, citing concerns about the Russian government capitalizing access provided by Kaspersky products.[5]

Executives from Google, Facebook, and Twitter testified publicly for the first time on how Russia used their service platforms to interfere with the 2016 Presidential Election.[6] Earlier in October, the Senate introduced a bill, the Honest Ads Act, to improve transparency and accountability in online political ads, which include political ads on Facebook, Google, and

---

[1] *Sally Yates's Testimony Before Senate Judiciary Panel*, C-Span (May 8, 2017), https://www.c-span.org/video/?427577-1/white-house-warned-general-flynn-compromised.
[2] *Id.*
[3] Matthew Cole, et. al., *Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election*, The Intercept (June 5, 2017, 3:44 PM), https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/.
[4] Intelligence Authorization Act for Fiscal Year 2018, S. 1761, 115th Cong. (1st Sess. 2017), https://www.congress.gov/bill/115th-congress/senate-bill/1761/text#toc-id1B77F0E6176D44D8A4E89B2AD3F6EEAA.
[5] Statement, Dept. of Homeland Sec., DHS Statement on the Issuance of Binding Operational Directive 17-01 (Sept. 13, 2017), https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01.
[6] Mary Clare Jalonick & Barbara Ortutay, *Tech Companies Find More Signs of Russian Election Activity*, Chicago Tribune (Oct. 31, 2017, 11:16 AM), http://www.chicagotribune.com/news/nationworld/ct-facebook-russia-posts-20171030-story.html.

--

Twitter.[7] The bill, a direct response to Russian interference in the 2016 Presidential Election, would impose the same disclosure requirements for online ads as for TV and radio ads.[8] The Federal Election Commission also announced on October 10 that "in light of developments" it would reopen for public comment its disclosure rules for online political ads.[9]

State Voter Data by Presidential Election Commission

EPIC is fully engaged in the challenge of protecting democracy by promoting cybersecurity and election integrity. Notably, EPIC filed a case against the Presidential Election Commission concerning the unlawful collection of state voter data. EPIC filed suit to halt the Commission's collection of state voter data and to compel the Commission to conduct a Privacy Impact Assessment required by law.[10] EPIC's initial filing led the Commission to suspend the collection of voter data, discontinue the use of an unsafe computer server, and delete the state voter data that was unlawfully obtained. The lower court denied EPIC's motion for an injunction and EPIC appealed the preliminary decision. Oral arguments were heard on November 21, 2017, and EPIC is awaiting a determination from the U.S. Court of Appeals for the D.C. Circuit.

Uber Agrees to Stop Tracking Riders

Uber will end the practice of tracking customers before and after they are picked up.[11] In 2015, Uber announced the company would track the location of riders from the time they ordered a ride until after they had reached their destination.[12] EPIC promptly filed a complaint with the Federal Trade Commission (FTC) and stated that "This collection of user's information far exceeds what customers expect from the transportation service."[13] The end to Uber's tracking practice comes two weeks after Uber entered into a consent agreement with the FTC following a complaint filed EPIC that highlighted Uber's history of misusing customer data.[14] EPIC provided

---

[7] Press Release, Senator Amy Klobuchar, Klobuchar, Warner Announce Bipartisan Legislation Co-sponsored by McCain to Prevent Foreign Interference in Future Elections, Improve Transparency of Online Political Ads (Oct. 18, 2017), https://www.klobuchar.senate.gov/public/index.cfm/news-releases?ID=7F856C80-8553-4AB5-84DB-42F07080A90A.

[8] *See* Honest Ads Act, H.R. 4077, 115th Cong. (1st Sess. 2017); Honest Ads Act, S. 1989, 115th Cong. (1st Sess. 2017).

[9] Zainab Smith, *Advance NPRM on Internet Disclaimer Notices Reopened for Comment (2017)*, Fed. Election Comm. (Oct. 10, 2017), https://www.fec.gov/updates/advance-nprm-internet-disclaimer-notices-reopened-2017/.

[10] *See* Second Amend. Complaint, EPIC v. Presidential Advisory Comm'n, No. 17-1320 (D.C. Cir. 2017), https://epic.org/privacy/litigation/voter/epic-v-commission/EPIC-v-Commission-second-amended-complaint.pdf.

[11] Jim Puzzanghera, *Uber Says It'll Stop Tracking Riders After They're Dropped Off*, L.A. Times (Aug. 29, 2017), http://beta.latimes.com/business/la-fi-uber-location-privacy-20170829-story.html.

[12] Press Release, Katherine Tassi, Managing Counsel of Data Privacy, An Update on Privacy at Uber (May 28, 2017), https://newsroom.uber.com/an-update-on-privacy-at-uber/.

[13] EPIC Complaint, *In the Matter of Uber Technologies, Inc.*, Fed. Trade Comm'n (June 22, 2015), https://epic.org/privacy/internet/ftc/uber/Complaint.pdf.

[14] Press Release, Fed. Trade Comm'n, Uber Settles FTC Allegations that It Made Deceptive Privacy and Data Security Claims (Aug. 15, 2017), https://www.ftc.gov/news-events/press-releases/2017/08/uber-settles-ftc-allegations-it-made-deceptive-privacy-data.

--

detailed comments to the FTC urging the agency to strengthen the proposed settlement with Uber.[15] As with most FTC privacy settlements, the agreement also requires Uber to implement a comprehensive privacy program and obtain periodic independent third-party audits.

Internet-Connected Toys and Updated Guidance on COPPA

In early October, Mattel announced that it will scrap its plans to sell Aristotle, an Amazon Echo-type device that collects and stores data from young children.[16] The Campaign for a Commercial-Free Childhood (CFCC) sent a letter and 15,000 petition signatures to the toymaker, warning of privacy and childhood development concerns.[17] EPIC backed the CFCC campaign[18] and urged the Federal Trade Commission (FTC) in 2015 to regulate "always-on" Internet devices.[19]

The Federal Bureau of Investigations (FBI) released a Public Service Announcement warning consumers about privacy risks of internet-connected toys. "Smart toys and entertainment devices for children are increasingly incorporating technologies that learn and tailor their behaviors based on user interactions," the FBI wrote in the PSA, adding that the toys "could put the privacy and safety of children at risk due to the large amount of personal information that may be unwittingly disclosed."[20]

The FTC has updated its guidance for businesses on complying with the Children's Online Privacy Protection Act (COPPA).[21] The new guidance clarifies that connected toys, Internet of Things devices, and other products intended for children must comply with the Act.[22] The FTC has also clarified how the Children's Online Privacy Protection Act applies to toys that

---

[15] Comments of EPIC, *In the Matter of Uber, Inc.*, FTC File No. 152-3054 (Sept. 15, 2017), https://epic.org/apa/comments/EPIC-FTC-Uber-Settlement.pdf.
[16] Hayley Tsukayama, *Mattel Has Canceled Plans for a Kid-Focused AI Device That Drew Privacy Concerns*, Washington Post (Oct. 4, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/10/04/mattel-has-an-ai-device-to-soothe-babies-experts-are-begging-them-not-to-sell-it/?utm_term=.56d5cc51d01.
[17] Letter from Campaign for a Commercial-Free Childhood, to Margaret Georgiadis, CEO, Mattel, Inc. (Oct. 2, 2017), http://www.commercialfreechildhood.org/sites/default/files/Letter%20to%20Mattel.pdf.
[18] *Don't Let Mattel's New "Digital Nanny" Trade Children's Privacy for Profit*, CCFC, http://www.commercialfreechildhood.org/action/don't-let-mattels-new-digital-nanny-trade-childrens-privacy-profit#experts (quoting EPIC President Marc Rotenberg's opinion on Internet-connected toys).
[19] *EPIC Urges Investigation of "Always On" Consumer Devices*, EPIC.org (July 9, 2015), https://epic.org/2015/07/epic-urges-investigation-of-al.html.
[20] Public Service Announcement, Fed. Bureau of Investigation, Consumer Notice: Internet-Connected Could Present Privacy and Contact Concerns for Children (July 17, 2017), https://www.ic3.gov/media/2017/170717.aspx.
[21] *See Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business*, Fed. Trade Comm'n (June 2017), https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance.
[22] Kristin Cohen & Peder Magee, *FTC Updates COPPA Compliance Plan for Business*, Fed. Trade. Comm'n (June 21, 2017, 10:26 AM), https://www.ftc.gov/news-events/blogs/business-blog/2017/06/ftc-updates-coppa-compliance-plan-business.

--

make voice recordings of children.[23] The Commission's enforcement policy statement stated that an audio file may only be used "as a replacement for written words," and may only be maintained "for the brief time necessary for that purpose."[24] Additionally, "the operator may not make any other use of the audio file in the brief period before the file is destroyed — for example, for behavioral targeting or profiling purposes."

EPIC filed a complaint with the FTC in December 2016, alleging that toys My Friend Cayla and i-Que Intelligent Robot violate federal privacy laws.[25] The complaint spurred international efforts[26] to ban the toys from the marketplace and a congressional investigation[27] into the toy makers' data practices.

Lastly, EPIC and a coalition of leading consumer groups have asked the Consumer Product Safety Commission to recall the Google Home Mini "smart speaker."[28] The touchpad on the Google device is permanently set to "on" so that it records all conversations without a consumer's knowledge or consent. The consumer groups said that "as new risks to consumers arise in consumer products, it is the responsibility of the Consumer Product Safety Commission to respond."[29]

Policy Guidance for Data Aggregation Services

The Consumer Financial Protection Bureau recently set out guidance for financial services that aggregate consumer data.[30] The Bureau outlined Consumer Protection Principles that "express the Bureau's vision for realizing a robust, safe, and workable data aggregation market that gives consumers protection, usefulness, and value."[31]

---

[23] Press Release, Fed. Trade Comm'n, FTC Provides Additional Guidance on COPPA and Voice Recordings (Oct. 23, 2017), https://www.ftc.gov/news-events/press-releases/2017/10/ftc-provides-additional-guidance-coppa-voice-recordings.

[24] Statement, Fed. Trade Comm'n, Enforcement Policy Statement Regarding the Applicability of the COPPA Rule to the Collection and Use of Voice Recordings (Oct. 20, 2017), https://www.ftc.gov/system/files/documents/public_statements/1266473/coppa_policy_statement_audiorecordings.pdf.

[25] EPIC Complaint, *In re: Genesis Toys and Nuance Communications*, Fed. Trade Comm'n (Dec. 6, 2016), https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf.

[26] *See e.g.*, *Connected Toys Violate European Consumer Law*, ForbrukerRadet (Dec. 6, 2016), https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws.

[27] Press Release, Senator Ed Markey, Sen. Markey Queries Toymakers: How Do You Protect Children's Information? (Dec. 6, 2016), https://www.markey.senate.gov/news/press-releases/sen-markey-queries-toymakers-how-do-you-protect-childrens-information.

[28] Letter from EPIC, et. al., to Ann Marie Buerkle, Chairman, U.S. Consumer Product Safety Comm'n (Oct 13, 2017), https://epic.org/privacy/consumer/Letter-to-CPSC-re-Google-Mini-Oct-2017.pdf.

[29] *Id.*

[30] Consumer Fin. Prot. Bureau, Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation (2017), http://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.

[31] The Consumer Protection Principles for aggregated consumer data services are: (1) consumer access to information, (2) usability and limited scope of access by third parties, (3) consumer control and informed

--

II. United States Supreme Court

U.S. Supreme Court Overturns North Carolina's Ban on Social Media Use by Sex Offenders: *Packingham v. North Carolina*

In *Packingham v. North Carolina*, the U.S. Supreme Court held that a North Carolina state law barring people listed on a sex offender registry from access or using "social networking" websites violates the First Amendment.[32] The North Carolina law barred registered sex offenders from accessing commercial websites that allow minors to register and communicate, including major news sites such as the Washington Post and CNN. EPIC filed an amicus brief in the case, joined by 30 technical experts and legal scholars, explaining that the state law violated the right to receive information, censored vast amounts of speech unrelated to protecting minors, and encouraged widespread government monitoring of all internet users.[33] Justice Ginsburg quoted EPIC's brief at oral argument, and the justices' written opinions noted policies and studies cited in EPIC's brief.[34]

Cell Phone Location Data: *Carpenter v. United States*

The U.S. Supreme Court has granted review in *Carpenter v. United States*, a case concerning the privacy of cell phone location data. At issue is whether the warrantless search and seizure of historical cell-phone records revealing the location and movements of a cell-phone user is permitted under the Fourth Amendment. A lower court ruled that the Fourth Amendment does not require officers to get a warrant before they obtain location records from a cell phone provider.[35] The Court is set to hear the case this fall. EPIC, along with thirty-six technical experts and legal scholars, filed an amicus brief in the upcoming case supporting the application of the warrant standard to obtain location data and recommended that the Court extend Constitutional protection to cell phone data.[36]

Fourth Amendment: *Collins v. Virginia* and *Byrd v. United States*

The Supreme Court has agreed to review two Fourth Amendment car search cases. In *Collins v. Virginia*, the Court will decide whether police can search a vehicle parked in the driveway of a private home without first obtaining a warrant.[37] In *Byrd v. United States*, the

---

consent, (4) authorizing payments, (5) security (6) access transparency, (7) accuracy, (8) ability to dispute and resolve unauthorized access, and (9) efficient and effective accountability mechanisms.

[32] Packingham v. North Carolina, 137 S. Ct. 1730 (2017), https://www.supremecourt.gov/opinions/16pdf/15-1194_08l1.pdf.

[33] Brief for EPIC, et. al. as Amici Curiae Supporting Petitioner, Packingham v. North Carolina, 137 S. Ct. 1730 (2017) (No. 15-1194), https://epic.org/amicus/packingham/packingham-amicus-EPIC.pdf.

[34] Transcript of Oral Argument at 47, Packingham v. North Carolina, 137 S. Ct. 1730 (2017) (No. 15-1194), https://epic.org/amicus/packingham/packingham-oral-argument-transcript.pdf.

[35] U.S. v. Carpenter, 819 F.3d 88[0] (6th Cir. 2016).

[36] Brief for EPIC, et. al. as Amici Curiae Supporting Petitioner, Carpenter v. U.S., (2017) (No. 16-402), https://epic.org/amicus/location/carpenter/Carpenter-v-US-amicus-EPIC.pdf.

[37] Collins v. Commonwealth, 790 S.E.2d 611, 613 (2016), *cert. granted sub nom.* Collins v. Virginia, No. 16-1027, 2017 WL 736341 (U.S. Sept. 28, 2017).

--

Court will decide whether a person driving a rental car loses their expectation of privacy in the vehicle solely because they are not the official driver on the rental agreement.[38] EPIC filed a friend of the court brief in *Byrd v. United States* urging the Supreme Court to recognize that a modern car collects vast troves of personal data via a cell phone blue tooth connection.[39]

Communications Privacy: *United States v. Microsoft* and *Dahda v. United States*

The Supreme Court has agreed to review *United States v. Microsoft*, a landmark case about whether the U.S. government can force email providers to turn over users' private messages that are stored outside of the United States.[40] The government claims that the Electronic Communications Privacy Act allows investigators to demand emails from all over the world, in violation of national privacy laws. A federal appeals court rejected the government's arguments last year and ruled that Microsoft was not required to hand over emails that the company stores in Ireland.[41] The Supreme Court has also agreed to review *Dahda v. United States*, a related case about whether Title III of the Omnibus Crime Control and Safe Streets Act of 1968 require suppression of evidence obtained through a facially deficient wiretap order because it exceeds the judge's territorial jurisdiction.[42] Both cases are expected to be argued in early 2018.

III. Pending Federal Legislation

Consumer Privacy

Senators have introduced comprehensive legislation to protect consumers from data breach and identity theft.[43] The Consumer Privacy Protection Act of 2017 requires companies to provide notice to consumers after a data breach and meet certain baseline privacy and data security standards.[44] The Consumer Privacy Act also prohibits companies from using a data breach to force consumers into individual arbitration,[45] and would punish companies for concealing security breaches.

---

[38] United States v. Byrd, 679 F.'App'x 146 (3d Cir. 2017), *cert. granted*, No. 16-1371, 2017 WL 2119343 (U.S. Sept. 28, 2017).
[39] Brief for EPIC, et. al. as Amici Curiae Supporting Petitioner, Byrd v. U.S. (2017) (No. 16-1371), https://www.epic.org/amicus/fourth-amendment/byrd/Byrd-v-US-EPIC-Amicus-Brief.pdf.
[40] Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016), *cert. granted sub nom.* United States v. Microsoft Corp., No. 17-2, 2017 WL 2869958 (U.S. Oct. 16, 2017).
[41] *Id.*
[42] *United States v. Dahda*, 853 F.3d 1101, 1107 (10th Cir. 2017), *cert. granted*, No. 17-43, 2017 WL 2909270 (U.S. Oct. 16, 2017)
[43] Press Release, Senator Patrick Leahy, Leahy Introduces the Consumer Privacy Protection Act (Nov. 14, 2017), https://www.leahy.senate.gov/press/leahy-introduces-the-consumer-privacy-protection-act.
[44] The Consumer Privacy Protection Act of 2017, 115th Cong. (1st Sess. 2017), https://www.leahy.senate.gov/imo/media/doc/Consumer%20Privacy%20Protection%20Act.pdf.
[45] *Senate Response Forced Arbitration, Undermines Data Protection*, EPIC.org (Oct. 26, 2017), https://epic.org/2017/10/senate-restores-forced-arbitra.html.

--

The Browser Act is an act aimed at protecting online privacy.[46] The Browser Act would apply to Internet ISPs as well as Internet companies, such, as Google and Facebook, and would generally require "opt-in" consent before the collection or disclosure of sensitive information. The bill, however, lacks a private right of action or a remedy for violations, lacks data breach notification, and would overwrite stronger state privacy laws that protect consumers. The bill gives enforcement authority to the Federal Trade Commission, which has mostly failed to protect consumers online privacy.[47]

Cybersecurity and Internet of Things

Several Senators have introduced the Internet of Things (IoT) Cybersecurity Improvement Act of 2017.[48] The proposed legislation is aimed toward improving the security of Internet-connected devices, which is expected to include over 20 billion devices by 2020.[49] The bill would require "Internet of Things" devices purchased by the U.S. government to meet minimum security standards. IoT device manufacturers who sell products to the federal government must commit that their IoT devices: (1) are patchable; (2) do not contain known vulnerabilities; (3) rely on standard protocols; and (4) do not contain hard-coded passwords.

Automated Vehicles

Privacy safeguards for connected vehicles is now a global concern. During the 39th International Conference of Data Protection & Privacy Commissioners, privacy Officials from more than 40 countries adopted a resolution on Data Protection in Automated and Connected Vehicles urging all parties to "fully respect the users' rights to the protection of their personal data and privacy."[50]

The House of Representatives has passed the SELF DRIVE Act to encourage the deployment of "automated vehicles" in the United States.[51] Responding to widespread privacy concerns, the bill requires automated vehicle manufacturers to create "privacy plans" and asks the Federal Trade Commission to prepare a privacy study on the automated vehicle industry. The bill, however it does not address who owns the data collected by automated vehicles or how consumers can access or delete their data. The bill supports the development of "Privacy Enhancing Techniques," such as anonymization.

---

[46] The BROWSER Act of 2017, H.R. 2520, 115th Cong. (1st Sess. 2017).
[47] *See e.g.*, *In re Google Buzz*, EPIC.org, https://epic.org/privacy/ftc/googlebuzz/; *In re Facebook*, EPIC.org, https://epic.org/privacy/inrefacebook/.
[48] Internet of Things (IoT) Cybersecurity Improvement Act of 2017, S. 1691, 115th Cong. (1st Sess. 2017).
[49] Press release, Senator Mark R. Warner, Senators Introduce Bipartisan Legislation to Improve Cybersecurity of "Internet-of-Things" (IoT) Devices (Aug. 1, 2017), https://www.warner.senate.gov/public/index.cfm/pressreleases?ID=06A5E941-FBC3-4A63-B9B4-523E18DADB36.
[50] Int'l Conference of Data Protection and Privacy Comm'r, *Resolution on Data Protection in Automated and Connected Vehicles* (Sept. 29, 2017), https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-data-protection-in-automated-and-connected-vehicles-.pdf.
[51] SELF Drive Act, H.R. 3388, 115th Cong. (1st Sess. 2017).

--

But the SELF DRIVE Act lacks essential privacy and safety standards and would preempt stronger state laws. The bill prevents the states from issuing any rule or regulation that is not identical to a Federal Motor Vehicle Safety Standard, preventing states from issuing their own safety and privacy regulations to safeguard consumers. States could still, however, set rules on registration, licensing, liability, insurance, and safety inspections for automated vehicles.

The Senate Commerce Committee favorably reported the AV START Act, a bill that aims to facilitate the deployment of connected vehicles in the United States.[52] The Committee adopted an amendment that directs the National Highway Traffic Safety Administration to create a publicly accessible database to determine the personal data collected by connected cars, how that information is used, data minimization and retention practices, security measures, and privacy policies of car manufacturers.[53]

The National Highway Traffic Safety Administration released revised guidance for automated vehicles.[54] The modified guidance encourages manufacturers to develop best practices to minimize cybersecurity risks. However, the NHTSA guidance lacks mandatory standards and fails to safeguard privacy stating that the Federal Trade Commission is responsible for consumer privacy.[55] Previous NHTSA guidance established privacy standards and required developers to minimize data collection.[56]

Federal Commission on Evidence-Based Policymaking Releases Final Report

The Commission on Evidence-Based Policymaking, which was tasked with studying whether and how data across the federal government could be combined for policy research while protecting privacy, has issued its final report.[57] The Commission backs evidence-based policy, recommends new privacy safeguards including Privacy Enhancing Techniques, encourage broader use of statistical data, and recommends the creation of a National Secure Data Service. The National Secure Data Service would be "charged with facilitating access and ensuring protection of data for evidence-building."[58]

---

[52] AV START Act, S. 1885, 115th Cong. (1st Sess. 2017).
[53] Mark up by Senator Edward J. Markey, S. 1885, 115th Cong. (1st Sess. 2017), https://www.commerce.senate.gov/public/_cache/files/edf17575-8d05-4563-ac35-1233291db60b/BE7D5E9B90D7B16AF2B8788E56797783.s.1885-markey-1-modified-.pdf.
[54] U.S. Dep't of Transp., Automated Driving Systems 2.0: A Vision for Safety (2017), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf.
[55] *Automated Driving Systems*, Nat'l Highway Traffic Safety Admin, https://www.nhtsa.gov/manufacturers/automated-driving-systems.
[56] *See* U.S. Dep't of Transp., Federal Automated Vehicles Policy: Accelerating the Next Revolution in Roadway Safety (2016), https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf.
[57] *See* Comm'n on Evidence-Based Policymaking, The Promise of Evidence-Based Policymaking (2017), https://www.cep.gov/content/dam/cep/report/cep-final-report.pdf.
[58] *Commission on Evidence-Based Policymaking Releases Final Report*, Consortium of Social Science Ass'n (Sept. 19, 2017), http://www.cossa.org/2017/09/19/commission-on-evidence-based-policymaking-releases-final-report/.

--

In testimony before the Commission, EPIC President Marc Rotenberg promoted both innovative privacy safeguards and well informed public policy.[59] EPIC also filed comments with the Commission urging adoption of Privacy Enhancing Techniques, such as anonymization, that minimize or eliminate the collection of personal data.[60] Additionally, the National Academies of Sciences released a report earlier this year that examined how disparate federal data sources can be used for policy research while protecting privacy.[61]

The Congress is now acting on the report findings by introducing evidence-based policy legislation.[62] Both titled Foundations for Evidence-Based Policy Making Act of 2017, the two concurrent bills address several recommendations by the Commission's report, including requiring federal agencies to create evidence-building plans, appoint a Chief Evaluation Office to coordinate the activities within the agency, and establish an advisory committee on data for evidence building. The bills also incorporate the OPEN Government Data Act, which requires federal agencies to establish a data inventory and data catalogue and ensure maximum data availability while still respecting privacy and national security concerns. The bills, however, do not explicitly authorize the of a creation of a National Secure Data Service.

Border Surveillance: Drones, Biometric Identification

The Border Security for America Act would dramatically expand surveillance capabilities along the northern and southern borders of the U.S.[63] The bill seeks "to achieve situational awareness and operational control of the border," with unmanned aerial vehicles (drones), radar surveillance systems, license plate readers, and biometric databases. The bill would establish a biometric exit data system, combined with other Federal databases, at U.S. airports, seaports, and land ports. The Privacy Act normally limits the government's ability to collect personal data, but this bill would exempt the Department of Homeland Security from compliance with the Privacy Act.[64] Previous EPIC FOIA lawsuits have revealed that border surveillance by drones would capture imagery, data, and Wi-Fi data of US citizens.[65]

---

[59] *See* Marc Rotenberg, *Commission on Evidence-Based Policymaking: Privacy Perspectives*, before the Nat'l Academies of Science (Sept. 9, 2016), https://epic.org/privacy/wiretap/Rotenberg-CEBP-9-16.pdf.
[60] *See* Comments of EPIC to the Comm'n on Evidence-Based Policymaking (Nov. 14, 2016), https://epic.org/apa/comments/EPIC-CEP-RFC.pdf.
[61] Nat'l Academies of Sciences, Innovations in Federal Statistics: Combining Data Sources While Protecting Privacy (Robert M. Groves et. al. eds., 2017), https://www.nap.edu/catalog/24652/innovations-in-federal-statistics-combining-data-sources-while-protecting-privacy.
[62] *See* Foundations for Evidence-Based Policymaking Act of 2017, H.R. 4147, 115th Cong. (1st Sess. 2017); Foundations for Evidence-Based Policymaking Act of 2017, S. 2046, 115th Cong. (1st Sess. 2017).
[63] Border Security for America Act, H.R. 4548, 115th Cong. (1st Sess. 2017).
[64] *The Privacy Act of 1974*, EPIC.org, https://epic.org/privacy/1974act/.
[65] *See e.g.*, Spotlight on Surveillance (October 2014) – Drones: Eyes in the Sky, EPIC.org, https://epic.org/privacy/surveillance/spotlight/1014/drones.html; Ryan Gallagher, *DHS Considers Eavesdropping Tech for Spy Drones on Border*, Slate (Mar. 1, 2013, 5:49 PM), http://www.slate.com/blogs/future_tense/2013/03/01/eavesdropping_drones_may_be_next_for_border_surveillance_efforts_in_texas.html.

--

Congress is also considering bi-partisan drone bills to protect the ability of states and local government to safeguard privacy. The House's Drone Innovation Act[66] and the Senate's Drone Federalism Act[67] would ensure that Federal Aviation Administration regulations do not preempt legitimate interests of local state governments to protect personal privacy.

Earlier this year, EPIC submitted a statement[68] to the House Transportation Committee and a statement[69] to the Senate Commerce Committee to emphasize the unique privacy risks of drones. EPIC explained that the FAA has failed to establish necessary privacy safeguards and that the states must be free to protect privacy interests.

Section 702 of the Foreign Intelligence Surveillance Act (Collection on non-US Persons)

Section 702 of the Foreign Intelligence Surveillance Act (FISA) allows agencies — without a warrant and in a broad range of circumstances — to search for information about Americans among communications collected for foreign intelligence purposes. The National Security Agency announced that it will no longer acquire upstream "about" communications under Section 702 surveillance authority.[70] The FISA Court previously questioned these searches, but permitted them to continue after the NSA claimed that ending the program would be technologically infeasible.[71]

With the broader Section 702 authority set to expire this upcoming December, Congress has been introducing legislation to reform Section 702. One Senator, a former chair of the Senate Intelligence Committee, outlined reforms to Section 702 surveillance authority that would end permanently the NSA's "about" searches, expand the amicus role at the intelligence court, and require the continued sunsetting of FISA authorities created in the FISA Amendments Act of 2008.[72] Recently, two senators have introduced the USA Liberty Act to reform surveillance under Section 702.[73] The USA Liberty Act would close the "backdoor search" loophole by requiring a probable cause court order before the government can review the contents of

---

[66] Drone Innovation Act of 2017, H.R. 2930, 115th Cong. (1st Sess. 2017).
[67] Drone Federalism Act of 2017, S. 1272, 115th Cong. (1st Sess. 2017).
[68] Letter from EPIC to Bill Shuster, Chairman, U.S. House Comm. on Transp. & Infrastructure, and Peter A. DeFazio, Ranking Member, U.S. House Comm. on Transp. & Infrastructure (June 8, 2017), https://epic.org/testimony/congress/EPIC-HTI-FAAreauth-June2017.pdf.
[69] Letter from EPIC to John Thune, Chairman, U.S. Senate Comm. on Commerce, Science, & Transp., and Bill Nelson, Ranking Member, U.S. Senate Comm. on Commerce, Science, & Transp. (Mar. 13, 2017), https://epic.org/testimony/congress/EPIC-SCOM-Drones-Mar2017.pdf.
[70] Statement, Nat'l Sec. Agency, NSA Stops Certain Section 702 "Upstream" Activities (April 28, 2017), https://www.nsa.gov/news-features/press-room/statements/2017-04-28-702-statement.shtml.
[71] Memorandum Opinion of October 31, 2011 Submissions, U.S. Foreign Intelligence Surveillance Ct. (Nov. 2011), https://www.dni.gov/files/documents/November%202011%20Bates%20Opinion%20and%20Order%20Part%201.pdf.
[72] Press Release, Senator Dianne Feinstein, Feinstein: Section 702 Reauthorization Important, Needs Changes (June 9, 2017), https://www.feinstein.senate.gov/public/index.cfm/press-releases?id=01BB10C6-DEBA-4584-A391-C7015FA947E9.
[73] USA Liberty Act of 2017, 115th Cong. (1st Sess. 2017), https://www.leahy.senate.gov/imo/media/doc/USALibertyActText.pdf.

--

Americans' communications.[74] The USA Liberty Act also codifies the ban on collecting "about" communications, mandates the appointment of amicus curiae for review of the surveillance programs, and establishes new reporting requirements.[75]

Among other reforms, eleven Senators introduced the bipartisan USA Rights Act, which codifies the ban on collecting "about" communications, prohibits collection of domestic communications, expands the powers of the Privacy and Civil Liberties Oversight Board, and requires independent amicus review during the FISC's annual authorization.[76] The bill does not establish certain protections sought by Europeans during the recent Privacy Shield review.[77]

Coalitions, however, call for the end to warrantless Section 702 searches and call for public hearings of any surveillance reform proposals. EPIC and a coalition of over 50 organizations called on lawmakers to require federal agencies to obtain a probable cause warrant before searching foreign intelligence databases for information about U.S. citizens and residents.[78] Moreover, EPIC joined a coalition of privacy and civil liberty organizations urging the Senate Intelligence Committee to open to the public any markup hearing on proposals to reauthorize Section 702.[79] "To the greatest degree possible, the consideration of legislation pertaining to Section 702...Should take place in public," the groups made clear in the letter to Senate Intelligence Committee leaders.

The ODNI 2016 Transparency Report provides new details about government surveillance activities. According to the ODNI, there was a 10% increase in the use of "backdoor searches" under Section 702.[80] These searches occur when a government search targets a U.S. person under a law intended to permit only surveillance of non-US persons.

---

[74] Press Release, Senator Patrick Leahy, Senator Lee and Senator Leahy Introduce the USA Liberty Act in the Senate (Nov. 11, 2017), https://www.leahy.senate.gov/press/senator-lee-and-senator-leahy-introduce-the-usa-liberty-act-in-the-senate.

[75] *See* Press Release, Nat'l Sec. Agency, 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.

[76] Summary of USA Rights Act, Senator Ron Wyden, https://www.wyden.senate.gov/download/?id=DCD8D965-457A-42AF-84B5-0010C6E062CA&download=1.

[77] *See* Press Release, European Commission, EU-US Privacy Shield: First Review Shows It Works but Implementation Can Be Improved (Oct. 18, 2017), http://europa.eu/rapid/press-release_IP-17-3966_en.htm.

[78] Letter from EPIC, et. al., to Bob Goodlatte, Chairman, House Judiciary Comm., and John Conyers, Ranking Member, House Judiciary Comm. (Oct. 3, 2017), https://epic.org/privacy/surveillance/fisa/Section702Backdoor-CoalitionLetter.pdf.

[79] Letter from EPIC, et. al., to Richard Burr, Chairman, Senate Intelligence Comm., and Mark Warner, Ranking Member, Senate Intelligence Comm. (Oct. 20, 2017), https://s3.amazonaws.com/demandprogress/letters/2017-10-20_Letter_SSCI_Keep_702_Markup_Open.pdf.

[80] Statistical Transparency Report: Regarding the Use of National Security Authorities for Calendar Year 2016, Office of the Director of Nat'l Intelligence (2017), https://www.dni.gov/files/icotr/ic_transparecy_report_cy2016_5_2_17.pdf.

--

Privacy Act Exemptions and Federal Databases

The FBI has released a final rule claiming several Privacy Act Exemptions for the Next Generation Identification (NGI) System, a database that contains the biometric data of millions of Americans, much of which is unrelated to law enforcement.[81] In issuing the final rule the FBI repeatedly stated that exemptions would be used responsibly and in accordance with FBI policies and procedures. Through a FOIA lawsuit, EPIC obtained documents that revealed the NGI database contained an error rate of up to 20% on facial recognition searches.[82]

The Department of Justice (DOJ) has issued a final rule on its "Insider Threat" database, a program that allows federal agencies to gather virtually unlimited amounts of personal data on individuals based on broad and ambiguous standards.[83] The DOJ exempted itself from Privacy Act safeguards that would limit the collection of personal data, and allow individuals access to their information maintained by the federal agency.

The Customs and Border Protection (CBP) agency published a system of records notice for the "Intelligence Records System."[84] The agency proposes to exempt the database from many Privacy Act safeguards.[85] The database contains detailed personal data from social media and commercial data services. CBP will use the "Analytical Framework for Intelligence" to secretly profile and evaluate social media users.

IV. Reports and Studies

Future of Truth and Misinformation Online

The Pew Research Center released a report on how to address the spread of digital misinformation in the coming decade.[86] The report's respondents were evenly divided on whether technological advances in the coming decade will fix the problem of misinformation, or only compound it. EPIC President Marc Rotenberg told Pew, "The problem with online news is structural: There are too few gatekeepers, and the internet business model does not sustain quality journalism. The reason is simply that advertising revenue has been untethered from news production."[87] The prevalence of "fake news" was one of the most significant issues in the 2016 presidential election.

---

[81] 28 C.F.R. § 16.96 (2017).
[82] *See EPIC v. FBI – Next Generation Identification*, EPIC.org, https://epic.org/foia/fbi/ngi/.
[83] 28 C.F.R. § 16.137 (2017).
[84] DHS/CBP-024 Intelligence Records Systems (CIRS) System of Records, 82 Fed. Reg. 44198 (Sept. 21, 2017).
[85] Privacy Act of 1974: Implementation of Exemptions for "Department of Homeland Security (DHS)/U.S. Customs and Border Protection (CBP)-024 CBP Intelligence Records Systems (CIRS) System of Records, 82 Fed. Reg. 44124 (Sept. 21, 2017).
[86] Janna Anderson & Lee Rainie, Pew Research Ctr., The Future of Truth and Misinformation Online (2017), http://assets.pewresearch.org/wp-content/uploads/sites/14/2017/10/19095643/PI_2017.10.19_Future-of-Truth-and-Misinformation_FINAL.pdf.
[87] *Id.* at 32.

--

Future of Online Trust

The Pew Research Center released a report of its survey of experts on "The Fate of Online Trust in the Next Decade." Although nearly half (48%) of the over 1,000 respondents said that they expected online trust to increase, 24% predicted that online trust would decrease.[88]

Internet of Things

The Pew Research Center has released a report surveying experts about the security implications of the Internet of Things (IoT).[89] The survey found a broad consensus that growth in the IoT will bring with it an increased risk of real-world physical harm. "The essential problem is that it will be impractical for people to disconnect," said EPIC President Marc Rotenberg in the survey.[90] "Cars and homes will become increasingly dependent on internet connectivity. The likely consequence will be more catastrophic events."[91] But, many respondents expressed confidence that effective regulatory and technology-based remedies will make the IoT safer. The Association for Computing Machinery recently released a Statement of IoT Privacy and Security, which lists principles for protecting privacy and security in IoT devices.[92]

Police Body Cameras

In the largest study to date of police body cameras, a new report concluded that the use of cameras had no impact on police use of force and civilian complaints.[93] The working paper report is a result of a project in Washington, D.C. to assess the benefits of the body cameras worn by the Metropolitan Police Department.[94]

---

[88] Lee Rainie & Janna Anderson, *The Fate of Online Trust in the Next Decade*, Pew Research Ctr. (Aug. 10, 2017), http://www.pewinternet.org/2017/08/10/the-fate-of-online-trust-in-the-next-decade/.
[89] Lee Rainie & Janna Anderson, *The Internet of Things Connectivity Binge: What Are the Implications?*, Pew Research Center (June 6, 2017) http://www.pewinternet.org/2017/06/06/the-internet-of-things-connectivity-binge-what-are-the-implications/.
[90] *Id.*
[91] *Id.*
[92] Statement on Internet of Things Privacy and Security, ACM U.S. Public Policy Counsel & ACM Europe Council Policy Committee (June 1, 2017), http://www.acm.org/binaries/content/assets/public-policy/2017_joint_statement_iotprivacysecurity.pdf.
[93] David Yokum, et. al., *Evaluating the Effects of Police Body-Worn Cameras: A Randomized Controlled Trial* 11 (The Lab @ D.C., Working Paper Oct. 20, 2017), http://bwc.thelab.dc.gov/TheLabDC_MPD_BWC_Working_Paper_10.20.17.pdf.
[94] *About the Project*, The Lab @ D.C., http://bwc.thelab.dc.gov/about.html.

--

V. Other Privacy Developments

Equifax Data Breach Harms 143 Million U.S. Consumers

In one of the most serious data breaches in U.S. history, the credit records of more than 140 million consumers, maintained by Equifax, have been compromised.[95] Credit reports typically include social security numbers, driver's license information, and other personal data that make possible identity theft and financial fraud. EPIC President Marc Rotenberg testified in front of the Senate Banking Committee about the breach stating that consumers should have greater control of their information.[96] EPIC previously recommended that Congress strengthen privacy laws and require Privacy Enhancing Techniques that minimize or eliminate the collection of personal data. In 2011, EPIC testified before the House[97] and the Senate[98] on the specific risk of data breaches in the financial services sector.

Congress is responding to the unprecedented number of recent data breaches by introducing several pieces of pending legislation. The Data Broker Accountability and Transparency Act would allow consumers to access and correct their personal data and stop data brokers from using, disclosing, or selling their information for marketing purposes.[99] The bill also requires data brokers to develop comprehensive privacy and data security measures and provide "reasonable notice" in the event of a breach. There are several other bills pending that would similarly require companies to notify customers following a breach of personally identifiable information and maintain cybersecurity protections when handling sensitive data.[100]

---

[95] *Equifax Announces Cybersecurity Incident Involving Consumer Information*, Equifax (Sept. 7, 2017), https://www.equifaxsecurity2017.com/2017/09/07/equifax-announces-cybersecurity-incident-involving-consumer-information/.

[96] *Consumer Data Security and the Credit Bureaus: Hearing Before the S. Comm. on Banking, Housing, & Urban Affairs*, 115th Cong. (2017), https://www.banking.senate.gov/public/index.cfm/2017/10/consumer-data-security-and-the-credit-bureaus.

[97] *Cybersecurity and Data Protection in the Financial Sector: Hearing Before the House Comm. on Fin. Serv.*, 112th Cong. (2011), https://financialservices.house.gov/uploadedfiles/091411rotenberg.pdf.

[98] *Cybersecurity and Data Protection in the Financial Sector: Hearing Before the S. Comm. on Banking, Housing, & Urban Affairs*, 112th Cong. (2011), https://epic.org/privacy/testimony/EPIC_Senate_Banking_Testimony%20_6_21_11.pdf.

[99] Data Broker Accountability and Transparency Act of 2017, S. 1815, 115th Cong. (1st Sess. 2017).

[100] *See e.g.*, Cyber Breach Notification Act of 2017, H.R. 3975, 115th Cong. (1st Sess. 2017); Secure and Protect Americans' Data Act, H.R. 3896, 115th Cong. (1st Sess. 2017); Data Breach Accountability and Enforcement Act of 2017, S. 1900, 115th (1st Sess. 2017); Data Protection Act of 2017, H.R. 3904, 115th (1st Sess. 2017); Personal Data Notification and Protection Act of 2017, H.R. 3806, 115th (1st Sess. 2017).

--

Uber Concealed 2016 Data Breach Affecting 57 Million People

Uber announced that in 2016, the ride sharing company faced a massive data breach that affected approximately 57 million customers, including both drivers and riders.[101] The breach revealed names, email address, phone numbers, and about 600,000 U.S. driver license numbers. Uber did not report the incident to affected customers or regulators, but instead paid hackers $100,000 to delete the data and keep the breach quiet.[102]

Google to End Email Content Scanning

After a decade of controversy, Google announced that it will stop scanning the content of all Gmail for ads personalization.[103] Google stopped scanning e-mails for education in 2014 after a lawsuit charged that it violated wiretap laws.[104] Google faced similar allegations in many other cases in the United States and around the world.[105] EPIC warned about Google's e-mail scanning practices back in 2005.[106] Last year, EPIC filed a friend-of-the-court brief in a Massachusetts case, again objecting to Google's Gmail scanning.[107]

FEC to Begin Rulemaking on Online Ad Transparency

After receiving over 150,000 public comments, the Federal Election Commission (FEC) voted unanimously to make new rules governing online political ad disclosures.[108] EPIC, numerous other organizations, and lawmakers pressed the FEC to require

---

[101] Press Release, Dara Khosrowshahi, CEO, Uber, 2016 Data Security Incident (Nov. 21, 2017), https://www.uber.com/newsroom/2016-data-incident/.
[102] Eric Newcomer, *Uber Paid Hackers to Delete Stolen Data on 57 Million People*, Bloomberg Tech. (Nov. 21, 2017, 6:19 PM), https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data.
[103] Diane Greene, *As G Suite Gains Traction in the Enterprise, G Suite's Gmail and Consumer Gmail to More Closely Align*, Google (June 23, 2017), https://blog.google/products/gmail/g-suite-gains-traction-in-the-enterprise-g-suites-gmail-and-consumer-gmail-to-more-closely-align/.
[104] Joe Silver, *Google Ends "Creepy" Practice of Scanning Gmail Education Apps*, Ars Technica (April 30, 2014, 1:01 PM), https://arstechnica.com/tech-policy/2014/04/google-ends-creepy-practice-of-scanning-gmail-education-apps/.
[105] *See e.g.*, Claire Cain Miller, *Google Accused of Wiretapping in Gmail Scans*, N.Y. Times (Oct. 1, 2013), http://www.nytimes.com/2013/10/02/technology/google-accused-of-wiretapping-in-gmail-scans.html.
[106] *Privacy Risks of E-mail Scanning: Hearing Before the CA. S. Judiciary Comm.*, (CA 2005) (testimony of Chris Jay Hoofnagle, Director, EPIC West Coast Office), https://epic.org/privacy/gmail/casjud3.15.05.html.
[107] Brief for EPIC as Amici Curiae Supporting Plaintiff/Appellant, Marquis v. Google, Inc., 32 Mass. L. Rptr. 269 (SJC No. 12103) (2016), https://epic.org/amicus/massachusetts/google/EPIC-MA-Gmail-Amicus.pdf.
[108] John Eggerton, *FEC Opening New Inquiry Into 'Net Ad Disclosure*, Broadcasting & Cable (Nov. 16, 2017), http://www.broadcastingcable.com/news/washington/fec-opening-new-inquiry-net-ad-disclosures/170154.

--

transparency for online ads to combat foreign interference in U.S. elections.[109] The FEC had solicited public comments on its internet disclosure rules three times in six years before finally taking action. A group of 15 Senators wrote, "The FEC must close loopholes that have allowed foreign adversaries to sow discord and misinform the American electorate."[110] And a group of 18 members of Congress urged the FEC to "address head-on the topic of illicit foreign activity in U.S. elections."[111]

White House Vulnerability Review Process for Disclosing Tech Flaws

The White House has released the "Vulnerabilities Equities Policy and Process" (VEP), describing how the U.S. Government will make decisions regarding disclosure of "Zero-day vulnerabilities."[112] At issue are vulnerabilities in software and consumer products that can be exploited by intelligence agencies and malicious hackers. If the VEP review board — comprised of agency representatives such as the DHS, ODNI, CIA, FBI, OMB, Commerce Department, and NSA — votes for disclosure, the tech company will be notified "when possible" within 7 business days. The charter requires the NSA, serving as the board's secretariat, to produce an annual public report on VEP decisions.

VI. EPIC's Work

EPIC Launches Campaign to End FCC Data Retention Mandate

EPIC launched the "My Calls, My Data" campaign urging the public to support a proposal to end the FCC's data retention mandate.[113] The 1986 regulation requires telephone companies to keep the telephone numbers dialed, date, time, and call length of all U.S. telephone customers for an 18-month period.[114] An EPIC-led coalition filed a petition in 2015 calling for repeal of the rule, saying that the FCC's mandate "violates the fundamental right to privacy, exposes consumers to data breaches, stifles innovation, and reduces competition."

EPIC Launches "51 Reasons - Protect Voter Data"

---

[109] *See e.g.*, EPIC, Comment Letter on Reopening of Comment Period for Internet Communication Disclaimers, Notice 2017-12 (Nov. 3, 2017), https://epic.org/algorithmic-transparency/EPIC-FEC-PoliticalAds-Nov2017.pdf.

[110] Press Release, Senator Mark R. Warner, Senator Urge FEC to Improve Transparency for Online Ads (Nov. 13, 2017), https://www.warner.senate.gov/public/index.cfm/pressreleases?ID=4E0AF8CB-4AA0-4FBB-86DD-7E770242542A.

[111] Letter from John Sarbanes, Rep. for Maryland, et. al., to Neven F. Stipanovic, Acting Asst. Gen. Counsel, Fed. Election Comm'n (Nov. 9, 2017), https://sarbanes.house.gov/sites/sarbanes.house.gov/files/House_Internet_Disclaimers_FEC_Comment_Reg_2011-02_Nov2017.pdf.

[112] White House, Vulnerabilities Equities Policy and Process for the United States Government (Nov. 15, 2017), https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.

[113] *END the FCC Data Retention Mandate!*, EPIC.org, https://epic.org/privacy/fcc-data-retention/.

[114] Retention of Telephone Toll Records, 47 C.F.R. § 42.6 (2000).

--

EPIC launched "51 Reasons to End the Collection of State Voter Records by the Presidential Election Commission,"[115] in response to the request from the Presidential Commission on Election Integrity for state voter records.[116] The website includes comments from state election officials, specialists in election integrity, news organizations, voters, and public officials across the country, who have described the Commission's plan as "unlawful," "politicized," "unprecedented," "naive," "crazy," "ill-conceived," "poorly executed," "outrageous," and "a breach of trust with voters." In EPIC v. Commission, EPIC is seeking to end the Commission's collection of personal data of registered voters.[117]

EPIC Hosts Public Voice Event with NGOs and Privacy Commissioners

On September 25, 2017, EPIC and other NGOs held a Public Voice event at the 39th International Conference of Data Protection and Privacy Commissioners in Hong Kong.[118] Titled "Emerging Privacy Issues: A Dialogue Between NGOs & DPAs," the event addressed emerging privacy issues, including biometric identification, Algorithmic transparency, border surveillance, the India privacy decision, and implementation of the General Data Protection Regulation.

Recent EPIC Publications

Commentaries

Alan Butler, *Top Experts: Can Facebook Legally Disclose Russian Ads–What does the Stored Communications Act say?*, JUST SECURITY (2017-10-27)[119]

Marc Rotenberg, *Let's Use Government Data to Make Better Policy*, SCIENTIFIC AMERICAN (October 4, 2017)[120]

Marc Rotenberg, *Facebook's Privacy Hokey-Pokey*, FORTUNE (September 27, 2017)[121]

Marc Rotenberg, *Equifax, the Credit Reporting Industry, and What Congress Should Do Next*, HARVARD BUSINESS REVIEW (September 20, 2017)[122]

Marc Rotenberg, *Trump's Double Standard When It Comes to Privacy*, NEWSWEEK (September 16, 2017)[123]

---

[115] *Protect Voter Data*, EPIC.org, https://epic.org/voter-data/.
[116] *Voter Privacy and the Presidential Election*, EPIC.org, https://epic.org/privacy/voting/pacei/.
[117] *EPIC v. Presidential Election Commission*, EPIC.org, https://epic.org/privacy/litigation/voter/epic-v-commission/.
[118] *Emerging Privacy Issues: A Dialogue Between NGOs & DPA*, Public Voice (Sept. 25, 2017), http://thepublicvoice.org/events/hongkong17/.
[119] https://www.justsecurity.org/46347/expert-views-facebook-legally-disclose-russian-ads-stored-communications-act-1986/.
[120] https://blogs.scientificamerican.com/observations/let-rsquo-s-use-government-data-to-make-better-policy/.
[121] http://fortune.com/2017/09/22/facebook-russian-ads-fake-news-zuckerberg/.
[122] https://hbr.org/2017/09/equifax-the-credit-reporting-industry-and-what-congress-should-do-next.

--

Marc Rotenberg, *Trump and Privacy*, WASHINGTON SPECTATOR (September 14, 2017)[124]

Alan Butler, *Symposium: Millions of tiny constables – Time to set the record straight on the Fourth Amendment and location-data privacy*, SCOTUSBLOG (August 3, 2017)[125]

Jeramie D. Scott, *Facial recognition surveillance is here — but privacy protections are not*, THE HILL (July 13, 2017)[126]

Jeramie D. Scott, *Social Media and Government Surveillance: The Case for Better Privacy Protections for Our Newest Public Space*, 12 J. BUS. & TECH. L. 151 (2017)[127]

Marc Rotenberg, *Data Driven*, THE ECONOMIST (May 25, 2017)[128]

Books

EPIC Bookstore – with many books by members of the EPIC Advisory Board and other featured authors – www.epic.org/bookstore

Privacy Law Sourcebook 2016: United States Law, International Law, and Recent Developments (Kindle Edition), edited by Marc Rotenberg (EPIC 2016)

Privacy and Human Rights (Kindle Edition): An International Survey of Privacy Laws and Developments, edited by Marc Rotenberg (EPIC 2016)

Communications Law and Policy: Cases and Materials, 5th Edition, by Jerry Kang and Alan Butler (Direct Injection Press 2016)

Privacy Law and Society, 3rd Edition, by Anita L. Allen and Marc Rotenberg (West 2015)

Privacy in the Modern Age: The Search for Solutions, by Marc Rotenberg, Julia Horwitz, and Jeramie Scott (The New Press 2015).

Privacy in the Modern Age: The Search for Solutions, Chinese Edition, by Marc Rotenberg, Julia Horwitz, and Jeramie Scott (The New Press 2015).

Further information about privacy developments in the United States is available at the Electronic Privacy Information Center's website – www.epic.org. For biweekly updates, subscribe to the EPIC Alert.

---

[123] http://www.newsweek.com/trumps-double-standard-when-it-comes-privacy-666234.
[124] https://washingtonspectator.org/rotenberg-trump-privacy/.
[125] http://www.scotusblog.com/2017/08/symposium-millions-tiny-constables-time-set-record-straight-fourth-amendment-location-data-privacy/.
[126] http://thehill.com/blogs/pundits-blog/technology/341906-opinion-facial-recognition-surveillance-is-here-but-privacy.
[127] http://digitalcommons.law.umaryland.edu/jbtl/vol12/iss2/2/.
[128] https://www.economist.com/news/letters/21722605-data-france-poland-and-more-letters-editor.

--

Appendix: EPIC Resources for 62nd IWG

Connected vehicles, EPIC comments to the Federal Trade Commission (May 1, 2017): https://epic.org/apa/comments/EPIC-ConnectedCar-Workshop-Comments.pdf

Video Privacy Act, EPIC amicus brief to 11th Circuit Court of Appeals, *Perry v. CNN* (July 22, 2016): https://epic.org/amicus/vppa/perry/EPIC-Amicus-Brief-Perry.pdf

Common carrier FTC exemption, EPIC amicus brief to 9th Circuit Court of Appeals, *FTC v. AT&T Mobility* (Oct. 24, 2016): https://epic.org/privacy/ftc/Consumer-Org-FTC-Common-Carrier-Amicus.pdf

Algorithmic transparency, EPIC complaint to the Federal Trade Commission (May 17, 2017): https://epic.org/algorithmic-transparency/EPIC-FTC-UTR-Complaint.pdf

Collection of social media identifiers for Visa applicants, EPIC comments to the State Department (May 18, 2017): https://epic.org/apa/comments/EPIC-DOS-Social-Media-ID-Collection-Comments.pdf

Privacy Act exemptions, EPIC comments to Department of Homeland Security (June 5, 2017): https://epic.org/apa/comments/EPIC-DHS-FALCON-Database-Comments.pdf

Eliminating robocalls, EPIC comments to Federal Communication Commission (June 30, 2017): https://epic.org/apa/comments/EPIC-FCC-Robocall-Comments.pdf

Biometric identifiers, EPIC comments to Transportation Security Administration (July 3, 2017): https://epic.org/apa/comments/EPIC-TSA-Pre-Check-Expansion-Comments.pdf

Privacy Act exemptions, EPIC comments to Department of Justice (June 30, 2017): https://epic.org/apa/comments/EPIC-DOJ-Insider-Threat-Database.pdf

Informational privacy and free association, EPIC amicus brief to 9th Circuit Court of Appeals, *Jane and John Doe 1-10 v. David Daleiden* (Mar. 16, 2017): https://epic.org/amicus/daleiden/EPIC-Amicus-Does-v-Daleiden.pdf

Privacy of Voter Data, EPIC advisory to state election officials (July 27, 2017): https://epic.org/privacy/litigation/voter/epic-v-commission/EPICAdvisory-EPICvCommission.pdf

Google tracking of in-store purchases, EPIC complaint to Federal Trade Commission (July 31, 2017): https://epic.org/privacy/ftc/google/EPIC-FTC-Google-Purchase-Tracking-Complaint.pdf

Consumer protection for data breach victims, EPIC amicus brief to federal appeals court in Washington, D.C., *Attias v. CareFirst* (Jan. 17, 2017): https://epic.org/amicus/data-breach/carefirst/EPIC-Amicus-Brief-Carefirst.pdf

--

Fourth Amendment and location data, EPIC amicus brief to the U.S. Supreme Court, *Carpenter v. United States* (Aug. 14, 2017): https://epic.org/amicus/location/carpenter/Carpenter-v-US-amicus-EPIC.pdf

Consumer protection for data breach victims, EPIC amicus brief to 8th Circuit Court of Appeals, *Alleruzzo v. SuperValu* (July 19, 2016): https://epic.org/amicus/data-breach/supervalu/EPIC-Amicus-SuperValu.pdf

CAN-SPAM Rule, EPIC comments to the Federal Trade Commission (Aug. 31, 2017): https://epic.org/apa/comments/EPIC-FTC-CAN-SPAM-Comments.pdf

License plate data are public records, EPIC amicus brief to California Supreme Court, *ACLU of Southern California v. Superior Court of Los Angeles* (May 6, 2016): https://epic.org/amicus/foia/california/alpr/EPIC-Amicus.pdf

SNN on Medicare ID Cards, EPIC testimony before U.S. Senate Committee on Aging (Oct. 7, 2015): https://epic.org/privacy/ssn/EPIC-SSN-Testimony-Senate-10-7-15.pdf

FTC Uber settlement, EPIC comments to the Federal Trade Commission (Sept. 15, 2017): https://epic.org/apa/comments/EPIC-FTC-Uber-Settlement.pdf

*Evidence-based policymakin*g, EPIC statement to U.S. House Committee on Oversight & Government Reform (Sept. 25, 2017): https://epic.org/testimony/congress/EPIC-HOGR-CEBP-Sep2017.pdf

Facebook tracking users, EPIC amicus brief to 9th Circuit Court of Appeals, *Smith v. Facebook* (Sept. 26, 2017): https://epic.org/amicus/facebook/smith/EPIC-Amicus-Brief-Smith-v-Facebook.pdf

Standing in video privacy case, EPIC letter brief to 9th Circuit Court of Appeals, *Eichenberger v. ESPN, Inc.* (Sept. 28, 2018): https://epic.org/amicus/vppa/eichenberger/Eichenberger-v-ESPN-EPIC-Amicus-Letter-Brief.pdf

User privacy case concerning "scraping of personal data," EPIC amicus brief to the 9th Circuit Court of Appeals, hiQ Labs, Inc. v. LinkedIn Corp. (Oct. 10, 2017): https://epic.org/amicus/cfaa/linkedin/hiQ-v-LinkedIn-EPIC-Amicus-Brief.pdf

Social media surveillance, EPIC comments to the Department of Homeland Security (Oct. 18, 2017): https://epic.org/apa/comments/EPIC-DHS-Social-Media-Info-Collection.pdf

Social media data collection, EPIC comments to the Custom and Border Protection (Oct. 23, 2017): https://epic.org/apa/comments/EPIC-CBP-Intelligence-Records-System-Comments.pdf

Assessing progress on commitment to transparency, EPIC comments to the Open Government Partnership's Independent Reporting Mechanism (Oct. 30, 2017): https://epic.org/open_gov/Comments_Progress_toward_NAP_20171030.pdf

--

Security at seaports, EPIC statement to House Homeland Security Committee (Oct. 30, 2017): https://epic.org/testimony/congress/EPIC-HHSC-Seaports-Oct2017.pdf

Informational injury, EPIC letter to the Federal Trade Commission (Oct. 31, 2017): https://epic.org/privacy/ftc/FTC-Letter-Informational-Injury-Workshop-10-24-17.pdf

Algorithmic transparency for political ads, EPIC comments to the Federal Election Commission (Nov. 3, 2017): https://www.epic.org/algorithmic-transparency/EPIC-FEC-PoliticalAds-Nov2017.pdf

FBI response to Russia attack, EPIC statement to House Judiciary Committee (Nov. 14, 2017): https://www.epic.org/testimony/congress/EPIC-HJC-Russia-Nov2017.pdf

Voluntary guidelines for autonomous vehicles, EPIC comments to the National Highway Traffic Safety Administration (Nov. 14, 2017): https://www.epic.org/apa/comments/EPIC-NHTSA-AutomatedDrivingSystems.pdf

Personal data sent to government agencies, EPIC statement to House Homeland Security Committee (Nov. 15, 2017): https://www.epic.org/testimony/congress/EPIC-HHSC-CyberThreatSharing-Nov2017.pdf

Warrantless vehicle searches, EPIC amicus brief to U.S. Supreme Court, *Byrd v. United States* (Nov. 20, 2017): https://www.epic.org/amicus/fourth-amendment/byrd/Byrd-v-US-EPIC-Amicus-Brief.pdf