epic.org ELECTRONIC PRIVACY INFORMATION CENTER

International Working Group on Data Protection in Telecommunications
59th meeting
Oslo, Norway 25 – 26 April 2016

Country Report
United States of America
(provided by EPIC)

I. Recent developments – Legal Framework

I.1 Enacted legislation

Judicial Redress Act on limited privacy protections for Europeans
In February 2016 President Obama signed into law the Judicial Redress Act that amends the Privacy Act of 1974. The Judicial Redress Act is intended to extend Privacy Act protection to non-U.S. citizens. However, the Act of 2015 establishes limited, conditional rights that my be withdraw by US officials, without judicial review, if the US government is not satisfied that the government of the individual seeking to enforce a right is cooperating with the United States. EPIC sent a letter to Congress, recommending substantial changes to the Judicial Redress Act to provide meaningful protections for data collected on non-U.S. persons.[1] EPIC explained that the legislation under consideration fails to provide adequate protection to permit transborder data flows. EPIC also pointed to increasing public concern in the United States about failure to enforce the law and the necessity of Privacy Act Modernization.

Cybersecurity Act of 2015 with significant surveillance implications[2]
The Cybersecurity Act of 2015 was signed into law by President Obama in December 2015.[3] The Cybersecurity Act was negotiated behind closed doors and represents a new version of the

[1] EPIC, Letter to the House Judiciary Committee on the Judicial Redress Act (Sept. 16, 2015), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf.
[2] Jenna McLaughlin, Last-Minute Budget Bill Allows New Privacy-Invading Surveillance in the Name of Cybersecurity, The Intercept (Dec. 18, 2016), Last-Minute Budget Bill Allows New Privacy-Invading Surveillance in the Name of Cybersecurity.
[3] Cybersecurity Act of 2015, https://epic.org/privacy/cybersecurity/Cybersecruity-Act-of-2015.pdf.

Cybersecurity Information Sharing Act (CISA). Previous versions of CISA have been opposed by a broad coalition of organizations who described the bill as the "Cyber Surveillance Act."[4] The law allows the government to obtain personal information from private companies without judicial oversight and it also expand government secrecy.[5] A key consideration regarding the implementation of the Act concerns the effectiveness of techniques that are intended to remove personally identifiable information.[6]

Evidence-Based Policy Commission with favorable privacy provisions

In March 2016 President Obama signed into law the Evidence-Based Policymaking Commission Act of 2016 to create a 15-member commission to work on the use of federal data without risking personal information privacy.[7] The task of the group is to establish ways to integrate rigorous evaluations of effectiveness—including randomized controlled trials—into the design of federal programs. At the same time, members will work on structures and policies must be in place to protect personal data during those evaluations. [8] The Commission would also study how best to protect the privacy rights of people who interact with federal agencies and ensure confidentiality. One-third of the Commission members are expected to be expert in "protecting personally-identifiable information and data minimization."

I.2 Legislative proposals

Federal Freedom of Information Act Reform

The Senate has passed the Freedom of Information Improvement Act of 2015.[9] The bill requires federal agencies to operate under a "presumption of openness." Senator Leahy, a co-sponsor of the bill, said that it "will help open the government to the 300 million Americans it serves and ensure that future administrations place an emphasis on openness and transparency."[10] The House passed a similar bill in January 2016.[11] Differences between the two versions must now be

[4] Coalition letter to oppose H.R. 1560,the Protecting Cyber Networks Act (Apr 21, 2015),https://www.aclu.org/sites/default/files/field_document/pcna_letter_final.pdf.
[5] Senator Patrick Leahy's Press Release, Government Transparency Will Take a Step Back Under Cyber Bill (Oct. 26, 2015), https://www.leahy.senate.gov/press/leahy-government-transparency-will-take-a-step-back-under-cyber-bill.
[6] Data Security Law Blog, "CISA is Now Law – What it Means for Your Organization," Jan. 29, 2016, http://datasecuritylaw.com/blog/cisa-is-now-law-what-it-means-for-your-organization/
[7] H.R. 1831 114th Congress (2016), Evidence-Based Policymaking Commission Act of 2016, https://www.govtrack.us/congress/bills/114/hr1831.
[8] Sarah D. Sparks, New Federal Commission on Evidence-Based Policymaking Approved by Obama (Mar 31, 2016), http://blogs.edweek.org/edweek/campaign-k-12/2016/03/obama_approves_commission_evidence.html.
[9] Freedom of Information Act Improvement Act of 2015, https://www.congress.gov/bill/114th-congress/senate-bill/337/text.
[10] Senator Patrick Leahy's Press Release, Leahy, Cornyn Bill Strengthening FOIA Passes Senate Unanimously (Mar 15, 2016), http://www.leahy.senate.gov/press/leahy-cornyn-bill-strengthening-foia-passes-senate-unanimously.
[11] H.R. 653 FOIA Act 114th Congress (2015), https://www.congress.gov/bill/114th-congress/house-bill/653/related-bills.

reconciled before President Obama can sign the bill into law. EPIC and a coalition of open government advocates urged the President to support the bipartisan legislation.[12]

Burr-Feinstein Anti-Encryption Bill

In April 2016 a legislative proposal to regulate encryption was published online. The bill would require that any "covered entity" that sells a product or method to "facilitate communication" is able to provide third-party access to the contents of those communications. This means that the bill would mandate those receiving a court order in an encryption case to provide "intelligible information or data" or the "technical means to get it" — in other words, a key to unlock secured data. EPIC joined the international coalition of NGOs in the Secure the Internet campaign to "reject policies that would prevent or undermine the use of strong encryption".[13]

Modest Email Privacy Updates[14]

A House Committee voted in favor of the Email Privacy Act, a bill that would amend the Electronic Communications Privacy Act of 1986 and establish a warrant requirement for the disclosure of all electronic communications.[15] A provision that would have required notice to the user of the search was removed in the revised bill. Senator Leahy, who has sponsored a similar bill in the Senate[16], said that "Congress has waited far too long to enact these reforms."[17] But the bill stops short of several updates recommended by EPIC, including protections for location data, data minimization requirements, and end-to-end encryption for commercial e-mail services.

II. Recent developments – Issues of Interest

Americans Strongly Favor Privacy, According to Pubic Opinion Polls

According to a January 2016 study of the Pew Research Center, "91% of adults agree or strongly agree that consumers have lost control of how personal information is collected and used by companies", "Americans express a consistent lack of confidence about the security of everyday communication channels and the organizations that control them", 74% say it is "very important"

[12] Coalition letter to President Obama on the Freedom of Information Act (Mar 16, 2016), http://www.openthegovernment.org/sites/default/files/Letter%20to%20the%20President%20-%20FOIA%20reform.pdf. *See also* www.foia.rocks.

[13] Secure the Internet (2016), https://www.securetheinternet.org/.

[14] EPIC's webpage on ECPA (2016), https://epic.org/privacy/ecpa/.

[15] H.R.699 114th Congress ,Email Privacy Act of 2016, https://www.congress.gov/bill/114th-congress/house-bill/699.

[16] S.356 Electronic Communications Privacy Act Amendments Act of 2015, https://www.congress.gov/bill/114th-congress/senate-bill/356.

[17] Press release, Comment of Senator Patrick Leahy (D-Vt.) and Senator Mike Lee (R-Utah) On the House Judiciary Committee Approving the Bipartisan Email Privacy Act (Apr 13, 2016),http://www.leahy.senate.gov/press/comment-of-senator-patrick-leahy-d-vt-and-senator-mike-lee-r-utah-on-the-house-judiciary-committee-approving-the-bipartisan-email-privacy-act-.

to them that they be in control of who can get information about them, and 65% say it is "very important" to them to control what information is collected about them.[18]

Data Breaches on the Rise

A new study of data breaches in the United States found a significant increase in the number of data breaches and the cost to companies. According to "2015 Cost of Data Breach Study: United States," the average cost for each lost or stolen record containing sensitive and confidential information increased from $201 to $217. The total average cost paid by organizations increased from $5.9 million to $6.5 million.[19] EPIC President Marc Rotenberg recently wrote in the *Wall Street Journal,* "Foreign corporations and governments would be negligent if they didn't consider the risks that result from the transfer of personal data."[20]

FCC Moves Forward With Narrow Privacy Rules

The Federal Communications Commission (FCC) has voted to adopt a Notice of Proposed Rulemaking on consumer privacy regulations.[21] The proposal follows Chairman Wheeler's earlier draft, which EPIC explained was too limited to safeguard online privacy.[22] During the vote, Commissioner Ajit Pai echoed EPIC's view that the rulemaking should not focus solely on ISPs.[23] EPIC previously urged the Commission to "address the full range of communications privacy issues facing US consumers" and to apply the Consumer Privacy Bill of Rights to communications data.[24]

Privacy Shield EU-U.S. Data Transfer Arrangement[25]

---

[18] Lee Rainie, The State of Privacy in America: What We Learned, Pew Research Center (Jan 20, 2016), http://www.pewresearch.org/fact-tank/2016/01/20/the-state-of-privacy-in-america/.

[19] Ponemon Institute, "2015 Cost of Data Breach Study: United States," (May 2015), http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEW03055USEN&appname=WWWSEARCH

[20] Marc Rotenberg, "They're Right to Distrust U.S. Data Security
Foreign corporations and governments would be negligent if they didn't consider the risks that result from the transfer of personal data to the U.S," *The Wall Street Journal*, Mar. 22, 2016, available at http://www.wsj.com/articles/theyre-right-to-distrust-u-s-data-security-1458655998?cb=logged0.5259012668648132&cb=logged0.12830793478045588

[21] FCC proposes Broadband Consumer Privacy Rules (Mar 31, 2016), https://www.fcc.gov/document/fcc-proposes-broadband-consumer-privacy-rules.

[22] EPIC's analysis on the FCC Communications Privacy Rulemaking (Mar 18, 2016), https://epic.org/privacy/consumer/EPIC-Draft-FCC-Privacy-Rules.pdf.

[23] The FCC's official website about Commissioner Ajit Pai (2016), https://www.fcc.gov/about/leadership/ajit-pai.

[24] EPIC, "Consumer Privacy Bill of Rights." https://epic.org/privacy/white_house_consumer_privacy_.html.

[25] EPIC's webpage on the Privacy Shield EU-U.S. Data Transfer Arrangement (2016), https://www.epic.org/privacy/intl/privacy-shield/.

On February 29, 2016, the European Commission and the US Commerce Department released the proposed EU-U.S. Privacy Shield. The Privacy Shield aims to replace the Safe Harbor framework for commercial data flows between the EU and the U.S., which was struck down by the Court of Justice of the European Union in October 2015. The Privacy Shield agreement is to serve as the basis for an "adequacy" decision by the European Commission that the U.S. has an "essentially equivalent" systems for data protection, including safeguards for government surveillance and consumer privacy. The Article 29 Working Party opinion on the Privacy Shield, released on April 13, 2016, indicates that the current draft of the Privacy Shield is not sufficient to satisfy the adequacy determination.[26]

In an earlier letter to Commissioner Vera Jourova and Secretary Penny Pritzker, EPIC and more than 40 NGOs urged the U.S. and the EU to protect the fundamental right to privacy. The groups warned that that without significant changes to "domestic law" and "international commitments," a new framework will almost certainly fail.[27] EPIC requested the establishment of an independent privacy agency in the U.S. and the adoption of a comprehensive privacy legislation to protect American consumers. EPIC and a coalition of NGOs called on the European Union, and the Article 29 Working Party in particular, to oppose the Privacy Shield proposal because the political agreement does not respect the decision of the European Court of Justice in the Schrems case.[28]

EPIC's President Marc Rotenberg in a testimony before the LIBE Committee of the European Parliament outlined several flaws in the proposed EU-US data transfer agreement, including a weak privacy framework, lack of enforcement, and a cumbersome redress mechanism. In the short term, Rotenberg recommended that the EU condition acceptance of the Privacy Shield on the end of the "702 program," which permits bulk surveillance on Europeans by the US. [29]

Transatlantic Consumer Dialogue's Advocacy about Privacy Shield
In April 2016, The Transatlantic Consumer Dialogue, a coalition of 70 NGOs in the EU and North America, issued a resolution to urge the negotiators to rewrite the Privacy Shield proposal

---

[26] Article 29 Working Party opinion on the Privacy Shield (Apr 13, 2016) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf, and Article 29 Working Party, Working document on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring data (European Essential Guarantees), (Apr 13, 2016) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf. See Mark Scott, "Europe's Privacy Watchdogs Call for Changes to U.S. Data-Transfer Deal," N.Y. Times, April 13, 2016, available at http://www.nytimes.com/2016/04/14/technology/europe-us-data-privacy.html

[27] NGO coalition letter to Commissioner Jourova and Secretary Pritzker (Nov 13, 2015), http://thepublicvoice.org/EU-US-NGO-letter-Safe-Harbor-11-15.pdf.

[28] NGO coalition letter to oppose the Privacy Shield proposal (Mar 16, 2016), https://epic.org/privacy/intl/schrems/Priv-Shield-Coalition-LtrMar2016.pdf.

[29] Marc Rotenberg, LIBE Hearing on Mar 17, 2016, http://www.europarl.europa.eu/ep-live/en/committees/video?event=20160317-1500-COMMITTEE-LIBE.

saying it fails to safeguard human rights and does not reflect changes in US law as required by the Schrems decision.[30]

U.S. Integration of Drones into the National Airspace, EPIC v. FAA

In February 2012, Congress passed the FAA Modernization and Reform Act and mandated that the Federal Aviation Administration create a comprehensive plan to integrate drones into the National Airspace.[31] Immediately afterwards, EPIC petitioned the FAA to perform a rulemaking on the privacy and civil liberty implications of domestic drones.[32] In 2014, the FAA denied EPIC's petition for a drone privacy rulemaking.[33] EPIC subsequently filed suit in the federal appeals court in Washington, DC arguing that the Federal Aviation Administration failed to establish privacy rules for commercial drones as mandated by Congress.[34] EPIC filed its opening brief in this case on September 28, 2015, charging that the agency's failure to establish privacy rules for commercial drones is a violation of law and should be overturned.[35] EPIC stated that "As the agency has determined not to issue rules, contrary to the FAA Modernization Act and EPIC's Rulemaking Petition, the Court must now order the agency to do so." The case is *EPIC v. FAA*, No. 15-1075. The United States Court of Appeals for the DC Circuit held oral argument in the case in February 2016. A decision is expected later this year. If it is favorable, the FAA will be required to establish a regulation requiring regulation of drone surveillance in the United States.

Apple v. FBI[36]

The dispute between Apple and the FBI arose out of an application that the agency filed with a federal magistrate judge in California, seeking assistance with the search of an iPhone that was seized during the investigation into the December 2015 attacks in San Bernardino, CA. The FBI claimed it was unable to access data on the locked iPhone, which was owned by the San Bernardino Health Department but used by one of the perpetrators, and requested that the Court order Apple to provide assistance in decrypting the phone. But because Apple has no way to access the encrypted data on the seized iPhone, the FBI applied for an order requiring Apple to create a custom operating system that would disable key security features on the iPhone. The Court issued an order requiring that this custom hacking tool be created and installed by Apple without unlocking or otherwise changing the data on the phone. Apple opposed the order on the grounds that it is unlawful and unconstitutional. Apple argued that if the order was granted it

[30] TACD Resolution on the Privacy Shield proposal (Apr 7, 2016), http://tacd.org/wp-content/uploads/2016/04/TACD-Resolution_Privacy-Shield_April163.pdf.
[31] The FAA Modernization and Reform Act of 2012, §§ 332(b)(2), 332(a)(1), Pub. L. 112-95, 126 Stat. 11, 73–75 (2012) (codified at 49 U.S.C. § 40101 note).
[32] Letter from EPIC, et al., to Michael P. Huerta, Acting Adm'r, Fed. Aviation Admin. (Mar. 8, 2012), available at https://epic.org/privacy/drones/FAA-553e-Petition-03-08-12.pdf.
[33] Letter from Fed. Aviation Admin. to EPIC (Nov. 26, 2014), available at https://epic.org/privacy/drones/FAA-Privacy-Rulemaking-Letter.pdf.
[34] EPIC v. FAA, No. 15-1075 (D.C. Cir. filed Mar. 31, 2015).
[35] Br. for Petitioner, EPIC v. FAA, No. 15-1075 (D.C. Cir.), available at https://epic.org/privacy/litigation/apa/faa/drones/1575326-EPIC-Opening-Brief.pdf.
[36] EPIC's webpage on Apple v. FBI (2016), https://epic.org/amicus/crypto/apple/.

would undermine the security of all Apple devices and set a dangerous precedent for future cases.

EPIC filed an amicus briefs in support of Apple's position, arguing that the Apple security techniques protected the privacy and security of cellphone users, and diminished the likely that third parties would gain access to the content of stolen phones, a growing concern among the American public[37] After strong public opposition to the government's conduct in the case, the FBI found a third-party that was able to unlock the iPhone without Apple's help and therefore asked the judge to drop the case.

FCC Set-top Box Proposal

The FCC is considering a proposal to open the set-top box market to third-party manufacturers, in a proceeding referred to as "Unlock the Box." The Notice of Proposed Rulemaking, formally titled "Expanding Consumers' Video Navigation Choices; Commercial Availability of Navigation Devices," would require cable companies to make cable programming available to third-party devices such as Roku and Apple TV.[38] The current proposal contains weak privacy protections for consumers' viewing habits, and would require third-party device manufacturers to self-certify compliance with privacy rules. EPIC has filed comments urging the FCC to strengthen enforcement of its cable privacy rules and to apply these rules to all parties with access to protected viewing data, including third-party device manufacturers.

III. Recent Developments – United States Supreme Court

Spokeo, INC. v. Robins[39]: Concerning whether courts have jurisdiction to review cases brought based on violations of federal statutory rights[40]

The Supreme Court will make a decision in an important privacy case concerning the disclosure of personal information in violation of the Fair Credit Reporting Act (FCRA).[41] *Spokeo v. Robins* arises from a data broker's publication of inaccurate, personal information in violation of the FCRA. The data broker, Spokeo, Inc., claimed that the plaintiff lacked "standing" to sue after the company disclosed data protected by the FCRA. EPIC filed an amicus brief for the Supreme Court defending Congress's authority to enact laws that safeguard the privacy of American consumers.[42] EPIC explained that "Congress enacted laws that establish rights for individuals and imposed obligations on the companies that profit from the collection and use of this data." Citing the current epidemic of privacy risks in the United States, including data breaches,

---

[37] EPIC and eight consumer privacy organizations' amicus brief in Apple v. FBI (Mar 3, 2016), https://epic.org/amicus/crypto/apple/EPIC-Corrected-Amicus-Brief.pdf.

[38] FCC proposal on "Expanding Consumers' Video Navigation Choices; Commercial Availability of Navigation Devices" (Feb 18, 2016) https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-18A1.pdf.

[39] Spokeo, Inc. v. Robins, No. 13-1339, http://www.supremecourt.gov/Search.aspx?FileName=/docketfiles/13-1339.htm

[40] Spokeo, Inc. v. Robins (2016), SCOTUSblog, http://www.scotusblog.com/case-files/cases/spokeo-inc-v-robins/.

[41] 15 U.S.C. § 1681 et seq.

[42] Br. of Amicus Curiae EPIC, *Spokeo v. Robins* (No. 13-1339), available at https://epic.org/amicus/spokeo/EPIC-Amicus-Brief.pdf.

identity theft, and financial fraud, EPIC wrote in the brief that this is "not the time for the Supreme Court to limit the ability of individuals to seek redress for violations of privacy rights set out by Congress." EPIC argued that plaintiffs can sue in federal court whenever a company misuses their personal information contrary to federal law.

Utah v. Strieff – Concerning whether Fourth Amendment allows evidence to be admitted after an illegal stop [43]

Mr. Strieff was unlawfully detained by an officer, who checked his ID and then arrested him on an unrelated outstanding warrant. In a brief, signed by twenty-one technical experts and legal scholars, EPIC detailed a number of sweeping government databases that contain inaccurate and detailed records about Americans' noncriminal activity. [44] EPIC warned about the vast amount of personal data, much of it inaccurate, stored in government databases and pointed to the failure of the Justice Department to enforce Privacy Act safeguards. The Supreme Court heard the case in February 2016.[45] A decision is expected by the end of June

IV. Recent Developments – EPIC's related work and upcoming events

10 Human Rights Organizations v. the United Kingdom at the European Court of Human Rights

EPIC filed a brief in the *10 Human Rights Organizations v the UK* (App. No. 24960/15) case before the European Court of Human Rights.[46] The case involves a challenge brought by 10 human rights organizations arguing that surveillance by British and U.S. intelligence organizations violated their fundamental rights.[47] In its brief, EPIC explained that the NSA's "technological capacities" enable "wide scale surveillance" and that U.S. statutes do not restrict surveillance of non-U.S. persons abroad. "The NSA collects personal data from around the world and transfer that data without adequate legal protections." This is EPIC's first brief for the European Court of Human Rights in Strasbourg.

"Data Protection 2016"

EPIC has launched a new campaign -- "Data Protection 2016" -- to support stronger privacy safeguards in the U.S.[48] The website www.dataprotection2016.org provides an overview of the data protection issue and proposes specific policy recommendations. The website includes an

---

[43] Utah v. Strieff, No.14-1373, http://www.supremecourt.gov/Search.aspx?FileName=/docketfiles/14-1373.htm.

[44] EPIC's amicus brief in Utah v. Strieff (Jan. 29, 2016), https://www.epic.org/amicus/strieff/EPIC-Amicus.pdf.

[45] Mark Joseph Stern, The First Day of the New Supreme Court, Slate (Feb. 23, 2016),http://www.slate.com/articles/news_and_politics/supreme_court_dispatches/2016/02/in_the_oral_arguments_for_utah_v_strieff_the_supreme_court_s_liberals_spoke.single.html.

[46] EPIC's brief in 10 Human Rights Organizations v the UK (Mar 18, 2016), https://epic.org/amicus/echr/liberty-gchq/TenHumanRightsOrganizations-EPIC-Amicus-ECtHR-18032016.pdf.

[47] EPIC's webpage on Liberty v. GCHQ (2016), https://epic.org/amicus/echr/liberty-gchq/.

[48] EPIC, Data Protection 2016 (2016), http://www.dataprotection2016.org/.

online store with campaign merchandise and links to affiliated sites. The campaign is non-partisan, and unaffiliated with the political parties.

EPIC Champions of Freedom Awards Dinner EPIC will host the 2016 Champions of Freedom Award dinner and ceremony on June 6, 2016 at the National Press Club in Washington, D.C. More information is available here: https://epic.org/june6/

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