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

March 22, 2017

The Honorable John Thune, Chairman
The Honorable Bill Nelson, Ranking Member
U.S. Senate Committee on Commerce, Science, & Transportation
512 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Thune and Ranking Member Nelson:

We write to you regarding the Committee's hearing on "The Promises and Perils of Emerging Technologies for Cybersecurity."[1] American consumers face unprecedented privacy and security threats. The unregulated collection of personal data and the growth of the Internet of Things has led to staggering increases in identity theft, security breaches, and financial fraud in the United States. Artificial Intelligence implicates a wide range of economic, social, and political issues in the United States. These issues have a significant impact on the future of cybersecurity, and we commend the Committee for exploring them.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[2] EPIC is a leading advocate for consumer privacy and has appeared before this Committee on several occasions.[3] EPIC is also focused on the impact of Artificial Intelligence (AI) on American society. In recent years, EPIC has opposed government use of "risk-based" profiling,[4] brought attention to the use of proprietary techniques for criminal

[1] *The Promises and Perils of Emerging Technologies for Cybersecurity*, 115th Cong. (2017), S. Comm. on Commerce, Science, and Transportation, http://www.commerce.senate.gov/public/index.cfm/hearings?ID=E0E0BBA1-231C-42A4-AF33-FC4DDFCF43C3 (March 22, 2017).

[2] *See* EPIC, *About EPIC*, https://epic.org/epic/about.html.

[3] *See, e.g,* Marc Rotenberg, EPIC Executive Director, Testimony before the U.S. Senate Committee on Commerce, Science, and Transportation, Commerce Committee, *Internet Privacy and Profiling* (June 13, 2000), https://epic.org/privacy/internet/senate-testimony.html; Letter from EPIC to the U.S. Senate Committee on Commerce, Science, and Transportation on Oversight of the FTC (Sept. 26, 2016), https://epic.org/privacy/consumer/EPIC-Letter-Sen- Comm-CST-FTC-Oversight.pdf; Letter from EPIC to the U.S. House of Representatives Committee on Energy and Commerce on FCC Privacy Rules (June 13, 2016), https://epic.org/privacy/consumer/EPIC-FCC-Privacy-Rules.pdf.

[4] EPIC et al., *Comments Urging the Department of Homeland Security To (A) Suspend the "Automated Targeting System" As Applied To Individuals, Or In the Alternative, (B) Fully Apply All Privacy Act Safeguards To Any Person Subject To the Automated Targeting System* (Dec. 4, 2006), *available at* http://epic.org/privacy/pdf/ats_comments.pdf; EPIC, *Comments on Automated Targeting System Notice of Privacy Act System of Records and Notice of Proposed Rulemaking*, Docket Nos. DHS-2007-0042 and DHS-2007-0043 (Sept. 5, 2007), *available at* http://epic.org/privacy/travel/ats/epic_090507.pdf. *See also*, *Automated Targeting System*, EPIC, https://epic.org/privacy/travel/ats/.

justice determinations,[5] and litigated several cases on the front lines of AI. In 2014, EPIC sued the U.S. Customs and Border Protection under the Freedom of Information Act ("FOIA") for documents about the use of secret tools to assign "risk assessments" to U.S. citizens.[6] EPIC also sued the Department of Homeland Security seeking documents related to a program that assesses "physiological and behavioral signals" to an individual's likelihood commit a crime.[7]

The Internet of Things Poses Numerous Privacy and Security Risks

The Internet of Things (IoT) poses significant privacy and security risks to American consumers.[8] The Internet of Things expands the ubiquitous collection of consumer data. This vast quantity of data could be used for purposes that are adverse to consumers, including remote surveillance. Smart devices also reveal a wealth of personal information about consumers, which companies may attempt to exploit by using it to target advertising or selling it directly. Because the IoT generates data from all aspects of consumers' daily existence, these types of secondary uses could lead to the commercialization of intimate segments of consumers' lives.

Many IoT devices feature "always on" tracking technology that surreptitiously records consumers' private conversations in their homes.[9] These "always on" devices raise numerous privacy concerns, including whether consumers have granted informed consent to this form of tracking. Even if the owner of an "always on" device has consented to constant, surreptitious tracking, a visitor to their home may not. Companies say that the devices rely on key words, but to detect those words, the devices must always be listening. And the key words are easily triggered. For example, several Amazon Echo devices treated a radio broadcast about the device as commands.[10] A San Diego television report about a girl using an Echo to order a $170 dollhouse and four pounds of sugar cookies triggered Echo devices across the city to make the same purchase.[11] A recent law enforcement request for Amazon Echo recordings[12] shows that "always on" devices will be much sought-after sources of information by law enforcement, foreign and domestic intelligence agencies, and, inevitably, cybercriminals.

---

[5] *EPIC Sues Justice Department Over "Risk Assessment" Techniques*, EPIC (March 7, 2017), https://epic.org/2017/03/epic-sues-justice-department-o.html (EPIC's Complaint against the DOJ is available at https://epic.org/foia/doj/criminal-justice-algorithms/EPIC-v-DOJ-criminal-justice-algorithms-complaint.pdf).

[6] *EPIC v. CBP (Analytical Framework for Intelligence)*, EPIC, https://epic.org/foia/dhs/cbp/afi/.

[7] *EPIC v. DHS – FAST Program*, EPIC, https://epic.org/foia/dhs/fast/.

[8] *See* Comments of EPIC to NTIA, *On the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things* (June 2, 2016), https://epic.org/apa/comments/EPIC-NTIA-on-IOT.pdf; *Internet of Things,* EPIC, https://epic.org/privacy/internet/iot/.

[9] EPIC Letter to DOJ Attorney General Loretta Lynch, FTC Chairwoman Edith Ramirez on "Always On" Devices (July 10, 2015), https://epic.org/privacy/internet/ftc/EPIC-Letter-FTC- AG-Always-On.pdf.

[10] Rachel Martin, *Listen Up: Your AI Assistant Goes Crazy For NPR Too*, NPR (Mar. 6, 2016), http://www.npr.org/2016/03/06/469383361/listen-up-your-ai-assistant-goes-crazy-for-npr-too.

[11] Carlos Correa, *News Anchor Sets off Alexa Devices Around San Diego Ordering Unwanted Dollhouses*, CW6 (Jan. 5, 2017), http://www.cw6sandiego.com/news-anchor-sets-off-alexa- devices-around-san-diego-ordering-unwanted-dollhouses/.

[12] *See* Christopher Mele, *Bid for Access to Amazon Echo Audio in Murder Case Raises Privacy Concerns*, N.Y. Times (Dec. 28, 2016), https://www.nytimes.com/2016/12/28/business/amazon- echo-murder-case-arkansas.html.

Another significant risk to consumers in the IoT is security, of both the users' data and their physical person. Many of the same security risks that currently threaten our data will only expand in the Internet of Things. The damage caused by malware, phishing, spam, and viruses will have an increasingly large array of networks in which to spread.[13] Additionally, not all wireless connections in the IoT are encrypted.[14] Researchers who studied encryption within the IoT found that "many of the devices exchanged personal or private information with servers on the Internet in the clear, completely unencrypted."[15]

In addition to data security risks, the IoT also poses risks to physical safety and personal property. This is particularly true given that the constant flow of data so easily delineates sensitive behavior patterns, and flows over networks that are not always secure, leaving consumers vulnerable to malicious hackers. For instance, a hacker could monitor Smart Grid power usage to determine when a consumer is at work, facilitating burglary, unauthorized entry, or worse. Researchers have already demonstrated the ability to hack into connected cars and control their operation, which poses potentially catastrophic risks to the public.[16]

It is not only the owners of IoT devices who suffer from the devices' poor security. The IoT has become a "botnet of things"—a massive network of compromised web cameras, digital video recorders, home routers, and other "smart devices" controlled by cybercriminals who use the botnet to take down web sites by overwhelming the sites with traffic from compromised devices.[17] The IoT was largely to blame for attacks in 2016 that knocked Twitter, Paypal, Reddit, Pinterest, and other popular websites off of the web for most of a day.[18] They were also behind the attack on security blogger Brian Krebs' web site, one of the largest attacks ever seen.[19]

These problems will not be solved by the market. Because poor IoT security is something that primarily affects other people, neither the manufacturers nor the owners of those devices have any incentive to fix weak security. Compromised devices still work fine, so most owners of devices that have been pulled into the "botnet of things" had no idea that their IP cameras,

---

[13] *See* EUROPEAN COMM'N, A DIGITAL AGENDA FOR EUROPE, 16-18 (2010), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF.

[14] Federal Motor Vehicle Safety Standards; Event Data Recorders, Docket No. NHTSA-2012-0177 (Comments of Privacy Coalition), 10 https://epic.org/privacy/edrs/EPIC-Coal-NHTSA-EDR-Cmts.pdf.

[15] Nick Feamster, *Who Will Secure the Internet of Things?*, FREEDOM TO TINKER (Jan. 19, 2016) https://freedom-to-tinker.com/blog/feamster/who-will-secure-the-internet-of-things/ (emphasis in original).

[16] *See, e.g.*, Karl Brauer & Akshay Anand, *Braking the Connected Car: The Future of Vehicle Vulnerabilities*, RSA Conference 2016, https://www.rsaconference.com/writable/presentations/file_upload/ht-t11-hacking-the-connected-car-thetfuturetof-vehicle-vulnerabilities.pdf ; FireEye, *Connected Cars: The Open Road for Hackers* (2016), https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/connected-cars-the-open-road-for-hackers.pdf.

[17] *See* Bruce Schneier, *We Need to Save the Internet from the Internet of Things*, Schneier on Security (Oct. 6, 2016), https://www.schneier.com/essays/archives/2016/10/we_need_to_save_the_.html

[18] *See* Scott Hilton, *Dyn Analysis Summary of Friday October 21 Attack*, Dyn.com (Oct. 26, 2016), http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/.

[19] *See* Brian Krebs, *KrebsOnSecurity Hit With Record DDoS*, KrebsOnSecurity (Sept. 21, 2016), https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/.

DVRs, and home routers are no longer under their own control. As Bruce Schneier said in recent congressional testimony, a manufacturer who puts a sticker on the box that says "This device costs $20 more and is 30 percent less likely to annoy people you don't know" probably will not get many sales.[20] We urge the Committee to address these numerous privacy and security concerns as it moves forward on legislation related to the Internet of Things.

The Challenge of AI

There is understandable enthusiasm about new techniques that promise medical breakthroughs, more efficient services, and new scientific outcomes. But there is also reason for caution. Computer scientist Joseph Weizenbaum famously illustrated the limitations of AI in the 1960s with the development of the Eliza program. The program extracted key phrases and mimicked human dialogue in the manner of non-directional psychotherapy. The user might enter, "I do not feel well today," to which the program would respond, "Why do you not feel well today?" Weizenbaum later argued in Computer Power and Human Reason that computers would likely gain enormous computational power but should not replace people because they lack such human qualities and compassion and wisdom.[21]

We face a similar reality today. EPIC has concluded that one of the primary public policy goals for AI must be "Algorithmic Transparency."[22]

The Need for Algorithmic Transparency

Democratic governance is built on principles of procedural fairness and transparency. And accountability is key to decision making. We must know the basis of decisions, whether right or wrong. But as decisions are automated, and we increasingly delegate decisionmaking to techniques we do not fully understand, processes become more opaque and less accountable. It is therefore imperative that algorithmic process be open, provable, and accountable. Arguments that algorithmic transparency is impossible or "too complex" are not reassuring. We must commit to this goal.

It is becoming increasingly clear that Congress must regulate AI to ensure accountability and transparency:

- Algorithms are often used to make adverse decisions about people. Algorithms deny people educational opportunities, employment, housing, insurance, and credit.[23] Many of these decisions are entirely opaque, leaving individuals to wonder whether the decisions were accurate, fair, or even about them.

[20] Testimony of Bruce Schneier before the House Committee on Energy & Commerce, Understanding the Role of Connected Devices in Recent Cyber Attacks, 114th Cong. (2016).
[21] Joseph Weizenbaum, *Computer Power and Human Reason: From Judgment to Calculation* (1976).
[22] *Algorithmic Transparency*, EPIC, https://epic.org/algorithmic-transparency/.
[23] Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1 (2014).

- Secret algorithms are deployed in the criminal justice system to assess forensic evidence, determine sentences, to even decide guilt or innocence.[24] Several states use proprietary commercial systems, not subject to open government laws, to determine guilt or innocence. The Model Penal Code recommends the implementation of recidivism-based actuarial instruments in sentencing guidelines.[25] But these systems, which defendants have no way to challenge are racially biased, unaccountable, and unreliable for forecasting violent crime.[26]

- Algorithms are used for social control. China's Communist Party is deploying a "social credit" system that assigns to each person government-determined favorability rating. "Infractions such as fare cheating, jaywalking, and violating family-planning rules" would affect a person's rating.[27] Low ratings are also assigned to those who frequent disfavored web sites or socialize with others who have low ratings. Citizens with low ratings will have trouble getting loans or government services. Citizens with high rating, assigned by the government, receive preferential treatment across a wide range of programs and activities.

- In the United States, U.S. Customs and Border Protection has used secret analytic tools to assign "risk assessments" to U.S. travelers.[28] These risk assessments, assigned by the U.S. government to U.S. citizens, raise fundamental questions about government accountability, due process, and fairness. They may also be taking us closer to the Chinese system of social control through AI.

EPIC believes that "Algorithmic Transparency" must be a fundamental principle for all AI-related work.[29] The phrase has both literal and figurative dimensions. In the literal sense, it is often necessary to determine the precise factors that contribute to a decision. If, for example, a government agency considers a factor such as race, gender, or religion to produce an adverse decision, then the decision-making process should be subject to scrutiny and the relevant factors identified.

Some have argued that algorithmic transparency is simply impossible, given the complexity and fluidity of modern processes. But if that is true, there must be some way to

[24] *EPIC v. DOJ (Criminal Justice Algorithms)*, EPIC, https://epic.org/foia/doj/criminal-justice-algorithms/; *Algorithms in the Criminal Justice System*, EPIC, https://epic.org/algorithmic-transparency/crim-justice/.
[25] Model Penal Code: Sentencing §6B.09 (Am. Law. Inst., Tentative Draft No. 2, 2011).
[26] *See* Julia Angwin et al., *Machine Bias*, ProPublica (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.
[27] Josh Chin & Gillian Wong, *China's New Tool for Social Control: A Credit Rating for Everything*, Wall Street J., Nov. 28, 2016, http://www.wsj.com/articles/chinas-new-tool-for- social-control-a-credit-rating-for-everything-1480351590
[28] *EPIC v. CBP* (Analytical Framework for Intelligence), EPIC, https://epic.org/foia/dhs/cbp/afi/.
[29] *At UNESCO, Rotenberg Argues for Algorithmic Transparency*, EPIC (Dec. 8, 2015), https://epic.org/2015/12/at-unesco-epics-rotenberg-argu.html.

recapture the purpose of transparency without simply relying on testing inputs and outputs. We have seen recently that it is almost trivial to design programs that evade testing.[30]

In the formulation of European data protection law, which follows from the U.S. Privacy Act of 1974, individuals have a right to access "the logic of the processing" concerning their personal information.[31] That principle is reflected in the transparency of the FICO score, which for many years remained a black box for consumers, making determinations about credit worthiness without any information provided to the customers about how to improve the score.[32]

Building on this core belief in algorithmic transparency, EPIC has urged public attention to four related principles to establish accountability for AI systems:

- "Stop Discrimination by Computer"
- "End Secret Profiling"
- "Open the Code"
- "Bayesian Determinations are not Justice"

The phrases are slogans, but they are also intended to provoke a policy debate and could provide the starting point for public policy for AI. And we would encourage you to consider how these themes could help frame future work by the Committee.

The continued deployment of AI-based systems raises profound issues for democratic countries. As Professor Frank Pasquale has said:

> Black box services are often wondrous to behold, but our black box society has become dangerously unstable, unfair, and unproductive. Neither New York quants nor California engineers can deliver a sound economy or a secure society. Those are the tasks of a citizenry, which can perform its job only as well as it understands the stakes.[33]

We ask that this letter be entered in the hearing record. EPIC looks forward to working with the Committee on these and other issues impacting the privacy and security of American consumers.

Sincerely,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President

/s/ Caitriona Fitzgerald
Caitriona Fitzgerald
EPIC Policy Director

---

[30] See Jack Ewing, *In '06 Slide Show, a Lesson in How VW Could Cheat*, N.Y. Times, Apr. 27, 2016, at A1.
[31] Directive 95/46/EC—The Data Protection Directive, art 15 (1), 1995, http://www.dataprotection.ie/docs/EU-Directive-95-46-EC--Chapter-2/93.htm.
[32] *See* Hadley Malcom, *Banks Compete on Free Credit Score Offers*, USA Today, Jan. 25, 2015, http://www.usatoday.com/story/money/2015/01/25/banks-free-credit-scores/22011803/.
[33] Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information* 218 (Harvard University Press 2015).