[For inclusion in the Hearing Record, Senate Commerce Committee, Nov. 30, 2016]

November 30, 2016

The Honorable Ted Cruz, Chairman
The Honorable Gary Peters, Ranking Member
U.S. Senate Committee on Commerce, Science, and Transportation
Subcommittee on Space, Science, and Competitiveness
512 Dirksen Senate Building
Washington, DC 20510

RE: Hearing on "The Dawn of Artificial Intelligence"

Dear Chairman Cruz and Ranking Member Peters:

We write to you regarding the upcoming hearing on "The Dawn of Artificial Intelligence."[1] We appreciate your interest in this topic. Artificial Intelligence implicates a wide range of economic, social, and political issues in the United States. As an organization now focused on the impact of Artificial Intelligence on American society, we submit this statement and ask that it be entered into the hearing record.

The Electronic Privacy Information Center ("EPIC") is a public interest research center established more than twenty years ago to focus public attention on emerging civil liberties issues. In recent years, EPIC has opposed government use of "risk-based" profiling,[2] brought attention to the use of proprietary techniques for criminal justice determinations, 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[3] EPIC also sued the Department of

[1] U.S. Senate Commerce, Science and Transportation Committee, Subcommittee on Space, Science, and Competitiveness, "The Dawn of Artificial Intelligence," (Nov. 30, 2016), http://www.commerce.senate.gov/public/index.cfm/hearings?ID=042DC718-9250-44C0-9BFE-E0371AFAEBAB

[2] 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/.

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

Homeland Security under the FPOA seeking documents related to a program that assesses "physiological and behavioral signals" to determine the probability that an individual might commit a crime.[4] Recently, EPIC appealed a Federal Aviation Administration final order for failing to establish privacy rules for commercial drones.[5]

EPIC has come to the conclusion that one of the primary public policy goals for AI must be "Algorithmic Transparency."[6]

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.[7]

We face a similar reality today.

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:

[4] EPIC, *EPIC v. DHS – FAST Program*, https://epic.org/foia/dhs/fast/. *See also* the film *Minority Report* (2002)

[5] EPIC, *EPIC v. FAA*, https://epic.org/privacy/litigation/apa/faa/drones/.

[6] EPIC, *Algorithmic Transparency*, https://epic.org/algorithmic-transparency/ (last visited Nov. 29, 2016). The web page contains an extensive collection of articles and commentaries by members of the EPIC Advisory Board, leading experts in law, technology, and public policy. More information about the EPIC Advisory Board is available at https://www.epic.org/epic/advisory_board.html.

[7] Joseph Weizenbaum, *Computer Power and Human Reason: From Judgment to Calculation* (1976).

- Algorithms are often used to make adverse decisions about people. Algorithms deny people educational opportunities, employment, housing, insurance, and credit.[8] Many of these decisions are entirely opaque, leaving individuals to wonder whether the decisions were accurate, fair, or even about them.

- Secret algorithms are deployed in the criminal justice system to assess forensic evidence, determine sentences, to even decide guilt or innocence.[9] 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.[10] But these systems, which defendants have no way to challenge are racially biased, unaccountable, and unreliable for forecasting violent crime.[11]

- 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. [12] 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.[13] 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.[14] 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

[8] Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1 (2014).

[9] EPIC, *Algorithms in the Criminal Justice System*, https://epic.org/algorithmic-transparency/crim-justice/ (last visited Nov. 29, 2016).

[10] Model Penal Code: Sentencing §6B.09 (Am. Law. Inst., Tentative Draft No. 2, 2011).

[11] *See* Julia Angwin et al., *Machine Bias*, ProPublica (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

[12] 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

[13] EPIC, *EPIC v. CBP (Analytical Framework for Intelligence)*, https://epic.org/foia/dhs/cbp/afi/ (last visited Nov. 29, 2016).

[14] EPIC, *At UNESCO, Rotenberg Argues for Algorithmic Transparency* (Dec. 8, 2015), https://epic.org/2015/12/at-unesco-epics-rotenberg-argu.html.

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 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.[15]

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.[16] 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.[17]

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.

Amending Asimov's Laws of Robotics

In 1942, Isaac Asimov introduced the "Three Laws of Robotics":

1. A robot may not injure a human being or, through inaction, allow a human being to come to harm.

2. A robot must obey the orders given it by human beings except where such orders would conflict with the First Law.

[15] *See* Jack Ewing, *In '06 Slide Show, a Lesson in How VW Could Cheat*, N.Y. Times, Apr. 27, 2016, at A1.
[16] 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.
[17] *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/.

3. A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws.[18]

Asimov's Rules of Robotics remain a staple of science fiction and ethical discourse.[19] But they also emerged in a time when the focus was on the physical ability of robots. In our present world, we have become increasingly aware that it is the accountability of autonomous devices that require the greater emphasis. For example, in seeking to establish privacy safeguards prior to the deployment of commercial drones in the United States,[20] EPIC became aware that drones would have an unprecedented ability to track and monitor individuals in physical space while remaining almost entirely anonymous to humans. Even the registration requirements established by the FAA would be of little practical benefit to an individual confronted by a drone in physical space.[21] Does the drone belong to a hobbyist, a criminal, or the police? Without basic identification information, it would be impossible to make this determination, even as the drone was able to determine the person's identity from a cell phone ID, facial recognition, speech recognition, or gait.[22]

This asymmetry poses a real threat. Along with the growing opacity of automated decision-making, it is the reason we have urged two amendments to Asimov's Laws of Robotics:

- A robot must always reveal the basis of its decision

- A robot must always reveal its actual identity

These insights also may be useful to the Committee as it explores the implications of Artificial Intelligence.

[18] Isaac Asimov, *Runaround*, Astounding Sci. Fiction, Mar. 1942, at 94.

[19] *See, e.g.*, Michael Idato, *Westworld's Producers Talk Artificial Intelligence, Isaac Asimov's Legacy and Rebooting a Cinematic Masterpiece for TV*, Sydney Morning Herald, Sept. 29, 2016, http://www.smh.com.au/entertainment/tv-and-radio/westworlds-producers-talk-artificial-intelligence-asimovs-legacy-and-rebooting-a-cinematic-masterpiece-for-tv-20160923-grn2yb.html ; George Dvorsky, *Why Asimov's Three Laws of Robotics Can't Protect Us*, Gizmodo (Mar. 28, 2014), http://io9.gizmodo.com/why-asimovs-three-laws-of-robotics-cant-protect-us-1553665410; TV Tropes, *Three-Laws Compliant*, http://tvtropes.org/pmwiki/pmwiki.php/Main/ThreeLawsCompliant (last visited Nov. 29, 2016).

[20] EPIC, *EPIC v. FAA*, https://epic.org/privacy/litigation/apa/faa/drones/ (last visited Nov. 29, 2016).

[21] Operation and Certification of Small Unmanned Aircraft Systems, 81 Fed. Reg. 42,064 (June 28, 2016) (to be codified at 14 CFR Parts 21, 43, 61, 91, 101, 107, 119, 133, and 183).

[22] *See, e.g.,* Jim Giles, *Cameras Know You by Your Walk*, New Scientist, Sept. 19, 2012, https://www.newscientist.com/article/mg21528835-600-cameras-know-you-by-your-walk/.

Conclusion

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.[23]

We appreciate your interest in this subject and urge the Committee to undertake a comprehensive review of this critical topic.

Sincerely,

Marc Rotenberg

Marc Rotenberg
EPIC President

James Graves

James Graves
EPIC Law and Technology Fellow

Enclosures

EPIC, "Algorithmic Transparency"

cc: The Honorable John Thune, Chairman, Senate Commerce Committee
The Honorable Bill Nelson, Ranking Member, Senate Commerce Committee

[23] Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information* 218 (Harvard University Press 2015).