epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

FEEDBACK OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

EUROPEAN COMMISSION INCEPTION IMPACT STATEMENT

Proposal for a legal act of the European Parliament and the Council laying down requirements for Artificial Intelligence

Sep. 10, 2020

EPIC submits the following feedback to the European Commission's Inception Impact Statement.[1] EPIC recommends that the Commission adopt subsection c of Option 3, requiring affirmative obligations and creating actionable consumer rights for all uses of AI. EPIC commends the Commission's efforts to regulate both public and private use of AI and to create uniform regulations throughout the European Union in order to avoid fragmented protection. However, EPIC urges the Union to introduce these regulations as a floor, allowing Member States to enact more stringent regulations as necessary to protect their citizens.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and human rights issues and to protect privacy, freedom of expression, and democratic values in the information age.[2] EPIC has a long history of promoting transparency and accountability for the use of automated decisionmaking systems and has consistently advocated for the adoption of the Universal Guidelines for AI ("UGAI") to promote trustworthy algorithms.[3] EPIC has litigated cases against the U.S. Department of Justice for

---

[1] European Commission Inception Impact Statement. *Artificial intelligence – ethical and legal* requirements, July 23, 2020, available at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Requirements-for-Artificial-Intelligence.

[2] EPIC, *About EPIC* (2019), https://epic.org/epic/about.html.

[3] *See* e.g. EPIC v. DOJ (D.C. Cir.) (18-5307), https://epic.org/foia/doj/criminal-justice-algorithms/; Comments of EPIC, *Intellectual Property Protection for Artificial Intelligence Innovation*, U.S. Patent and Trademark Office (Jan. 10, 2020), https://epic.org/apa/comments/EPIC-USPTO-Jan2020.pdf; Comments of EPIC, *HUD's Implementation of the Fair Housing Act's Disparate Impact Standard*, Department of Housing and Urban Development (Oct. 18, 2019), https://epic.org/apa/comments/EPIC-HUD-Oct2019.pdf; Testimony of EPIC, Massachusetts Joint Committee on the Judiciary (Oct. 22, 2019), https://epic.org/testimony/congress/EPIC-FacialRecognitionMoratorium-MA-Oct2019.pdf; Statement of EPIC, *Industries of the Future*, U.S. Senate Committee on Commerce, Science & Transportation (Jan. 15, 2020), https://epic.org/testimony/congress/EPIC-SCOM-AI-Jan2020.pdf; Comments of EPIC, *Request for Information: Big Data and the Future of Privacy*, Office of Science and Technology Policy (Apr. 4, 2014); EPIC, *Algorithmic Transparency* (2018), https://www.epic.org/algorithmic-transparency/; EPIC, *Algorithms in the Criminal Justice System* (2018), https://www.epic.org/algorithmic-transparency/crim-justice/;

documents regarding "risk assessment tools"[4] and against the U.S. Department of Homeland Security for documents about a program to assess the probability that an individual might commit a crime in the future.[5] In 2018, EPIC joined leading scientific societies to successfully petition the U.S. Office of Science and Technology Policy to solicit public input on U.S. Artificial Intelligence Policy.[6] EPIC also submitted comments urging the National Science Foundation to adopt the UGAI and to promote and enforce the UGAI across the funding, research, and deployment of AI systems.[7]

In an effort to safeguard consumers, EPIC recently filed complaints to the U.S. Federal Trade Commission regarding the business practices of HireVue,[8] an employment screening company, and AirBnB,[9] the lodging rental service that claims it can assess risk in potential renters based on an opaque algorithm. EPIC has also petitioned the FTC to regulate the use of AI in commerce.[10] EPIC recently published the *AI Policy Sourcebook*, the first comprehensive reference book on AI policy.[11]

EPIC recommends the Commission adopt the Universal Guidelines for AI and the OECD AI Principles as a baseline for AI regulation

EPIC provides specific feedback on the regulatory options posed by the Commission below. But, first, we summarize the the Universal Guidelines for Artificial Intelligence and the OECD AI Principles, which EPIC supports as the baseline for AI regulation.

The Universal Guidelines for Artificial Intelligence, a framework for AI governance based on the protection of human rights, were set out at the 2018 Public Voice meeting in Brussels, Belgium.[12] The Universal Guidelines have been endorsed by more than 250 experts and 60 organizations in 40 countries.[13] The UGAI comprise twelve principles:

Comments of EPIC, *Consumer Welfare Implications Associated with the Use of Algorithmic Decision Tools, Artificial Intelligence, and Predictive Analytics*, Federal Trade Commission (Aug. 20, 2018), https://epic.org/apa/comments/EPIC-FTC-Algorithmic-Transparency-Aug-20-2018.pdf; Comments of EPIC, *Developing UNESCO's Internet Universality Indicators: Help UNESCO Assess and Improve the Internet*, United Nations Educational, Scientific and Cultural Organization ("UNESCO") (Mar. 15, 2018), 5-6, https://epic.org/internetuniversality/EPIC_UNESCO_Internet_Universality_Comment%20(3).pdf. https://epic.org/privacy/big-data/EPIC-OSTP-Big-Data.pdf.

[4] EPIC, *EPIC v. DOJ (Criminal Justice Algorithms)* https://epic.org/foia/doj/criminal-justice-algorithms/.

[5] *See id.*; EPIC, *EPIC v. DHS (FAST Program)* https://epic.org/foia/dhs/fast/.

[6] EPIC, Petition to OSTP for Request for Information on Artificial Intelligence Policy (July 4, 2018), https://epic.org/privacy/ai/OSTP-AI-Petition.pdf.

[7] EPIC, Request for Information on Update to the 2016 National Artificial Intelligence Research and Development Strategic Plan, National Science Foundation, 83 FR 48655 (Oct. 26, 2018), https://epic.org/apa/comments/EPIC-Comments-NSF-AI-Strategic-Plan-2018.pdf.

[8] Complaint and Request for Investigation, Injunction, and Other Relief, *In re HireVue* (Nov. 6, 2019), https://epic.org/privacy/ftc/hirevue/EPIC_FTC_HireVue_Complaint.pdf.

[9] Complaint and Request for Investigation, Injunction, and Other Relief, *In re Airbnb* (Feb. 27, 2019), https://epic.org/privacy/ftc/airbnb/EPIC_FTC_Airbnb_Complaint_Feb2020.pdf.

[10] *In re: Petition for Rulemaking Concerning Use of Artificial Intelligence in Commerce*, EPIC (Feb. 3, 2020) https://epic.org/privacy/ftc/ai/EPIC-FTC-AI-Petition.pdf.

[11] *EPIC AI Policy Sourcebook 2020* (EPIC 2020), https://epic.org/bookstore/ai2020/.

[12] *Universal Guidelines for Artificial Intelligence*, The Public Voice (Oct. 23, 2018) [hereinafter *Universal Guidelines*], https://thepublicvoice.org/ai-universal-guidelines/

[13] *Id.*

1. Right to Transparency.
2. Right to Human Determination.
3. Identification Obligation.
4. Fairness Obligation.
5. Assessment and Accountability Obligation.
6. Accuracy, Reliability, and Validity Obligations.
7. Data Quality Obligation.
8. Public Safety Obligation.
9. Cybersecurity Obligation.
10. Prohibition on Secret Profiling.
11. Prohibition on Unitary Scoring.
12. Termination Obligation.[14]

The OECD AI Principles[15] were adopted in 2019 and endorsed by 42 countries—including several European Countries, the United States and the G20 nations.[16] The OECD AI Principles establish international standards for AI use:

1. Inclusive growth, sustainable development and well-being.
2. Human-centered values and fairness.
3. Transparency and explainability.
4. Robustness, security and safety.
5. Accountability.[17]

Options 0-2 are insufficient regulatory schemes in order to protect against the harms identified in the Impact Statement

Option 0, the baseline, and Option 1 are clearly insufficient to protect against the potential harms posed by AI systems.[18] There is already opportunity and encouragement to self-regulate throughout the world, but that alone is not effective in protecting consumers against the harms that AI systems create. Indeed, the harms defined in the Impact Statement have flourished under these

[14] *Id.*
[15] *Recommendation of the Council on Artificial Intelligence*, OECD (May 21, 2019) [hereinafter *OECD AI Principles*], https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449;
[16] *U.S. Joins with OECD in Adopting Global AI Principles*, NTIA (May 22, 2019), https://www.ntia.doc.gov/blog/2019/us-joins-oecd-adopting-global-ai-principles.
[17] *OECD AI Principles*, *supra* note 15.
[18] Option 0 indicates the option to not make any policy change in EU.
Option 1 uses a "soft law" approach, promoting self-regulation led by industry.
Option 2 would establish a voluntary labelling scheme for "trustworthy AI," that would allow developers to distinguish themselves to consumers.
Option 3 is legislation that establishes mandatory requirements about transparency, oversight, accuracy, and more. Subsection a-c offer legislation covering specific categories of AI (a), "high-risk" AI (b), and all uses of AI (c).
Option 4 offers a combination of the above options, using a risk-based approach to regulations.
Inception Impact Statement, *supra* note 1.

options. This is especially true in the United States, which has unsuccessfully pursued a self-regulatory model for the both AI and data processing systems.[19] The results have been disastrous.

For example, throughout the U.S. criminal justice system, the use of AI poses a high risk of violating fundamental rights. The use of predictive algorithms in facial recognition, drone surveillance, and other law enforcement contexts create acute risks. There is an inherent tendency to perpetuate policing patterns that already disproportionately disadvantage minorities. In pretrial dispositions, sentencing, and prisons, the use of algorithms to determine risk often leads to inaccurate, biased, or other improper results that exacerbate existing inequalities.[20] A study of facial recognition algorithms by the U.S. National Institute of Standards and Technology ("NIST") found the systems were up to 100 times more likely to return a false positive for a non-white person than for a white person.[21] Specifically, NIST found that "for one-to-many matching, the team saw higher rates of false positives for African American females," a finding that is "particularly important because the consequences could include false accusations."[22] A separate study by Stanford University and MIT, which looked at three widely deployed commercial facial recognition tools, found an error rate of 34.7% for dark-skinned women compared to an error rate of 0.8% for light-skinned men.[23] A review of Rekognition—an Amazon-owned facial recognition system marketed to law enforcement—revealed indications of racial bias and found that the system misidentified 28 members of U.S. Congress as convicted criminals.[24]

Systems that enable secret profiling of consumers using AI also present serious risks to fundamental rights. In 2017, Airbnb acquired Trooly, an AI risk assessment tool that can be used to rate potential guests[25] (or in the words of Trooly's patent, to "determin[e] trustworthiness and

---

[19] Karl Manheim and Lyric Kaplan, *Artificial Intelligence: Risks to Privacy and Democracy*, 21 Yale J. L. & Tech. 106, 110.

[20] *See, e.g.*, EPIC, *Algorithms in the Criminal Justice System: Pre-Trial Risk Assessment Tools* https://epic.org/algorithmic-transparency/crim-justice/; Melissa Hamilton, *The Biased Algorithm: Evidence of Disparate Impact on Hispanics*, 56 Am. Crim L. Rev. 1553 (2019), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3251763; Megan T. Stevenson & Christopher Slobogin, *Algorithmic Risk Assessments and the Double-Edged Sword of Youth*, 96 Wash. U.L. Rev. 681 (2018), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3225350; Julia Angwin et al., *Machine Bias*, ProPublica (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing; Tolan S., Miron M., Gomez E. and Castillo C. *Why Machine Learning May Lead to Unfairness: Evidence from Risk Assessment for Juvenile Justice in Catalonia*, Best Paper Award, International Conference on AI and Law, 2019.

[21] *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, Nat'l Inst. of Standards and Tech. (Dec. 19, 2019), https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.

[22] *Id*.

[23] Larry Hardesty, *Study finds gender and skin-type bias in commercial artificial-intelligence systems*, MIT News (Feb. 11, 2018), http://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212.

[24] Russell Brandom, *Amazon's facial recognition matched 28 members of Congress to criminal mugshots*, The Verge (Jul. 26, 2018) https://www.theverge.com/2018/7/26/17615634/amazon-rekognition-aclu-mug-shot-congress-facial-recognition.

[25] Mark Blunden, *Booker beware: Airbnb can scan your online life to see if you're a suitable guest*, Evening Standard (Jan. 3, 2020), https://www.standard.co.uk/tech/airbnb-software-scan-online-life-suitable-guest-a4325551.html.

compatibility of a person").[26] The AI system analyzes information collected from third parties—including service providers, blogs, public and commercial databases, and social networks—to generate a "trustworthiness" score.[27] The company claims that the system can identify whether an individual is involved with drugs or alcohol; hate websites or organizations; sex work and pornography; criminal activity; civil litigation; and fraud.[28] The company claims that the system can also identify "badness, anti-social tendencies, goodness, conscientiousness, openness, extraversion, agreeableness, neuroticism, narcissism, Machiavellianism, [and] psychopathy." AI systems such as HireVue that purport to detect subjective qualities for job applicants[29] are another risky form of consumer scoring.

The accuracy of systems like this are suspect because they are unaccountable and opaque. Furthermore, many of the "results" that these AI systems are designed to measure are highly subjective traits; there is no evidence that these traits can be accurately or fairly measured using an AI system. People may be unfairly denied housing, benefits, a job or other equal access to services based on subjective, opaque, and potentially inaccurate systems. These systems accordingly present a high risk to fundamental rights.

Option 2 is an improvement on Options 0–1 but risks further disadvantaging lower income earners and would not provide substantially improved protections for individuals. The optional labeling scheme could be harmful to consumers if companies merely leverage their designation as trustworthy as a justification to charge higher prices. Additionally, while optional labeling could be helpful in educating consumers about the risks associated with AI systems they affirmatively choose to use, the impact will be minimal because individuals typically have no knowledge of or control over the most harmful uses of AI. For example, predictive policing algorithms, emotion detection algorithms, and risk assessments used by both private and public actors are used against individuals without their willing participation.[30] As the Commission recognizes in the Inception Impact Statement: "biased and discriminatory outcomes resulting from decisions taken or supported by AI systems might remain completely unperceived or difficult to challenge without appropriate documentation about how the system works or about the goals it pursues."[31]

A key inadequacy of regulations is a lack of mandatory transparency about when automated decision-making systems are being used. An optional labeling system would not resolve this harm. The resources required to ensure the efficacy of a label system would be significant—and better allocated to affirmatively ameliorating the harms that these systems create.

---

[26] U.S. Patent No. 9,070,088 (filed June 30, 2015), *available at* http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=9070088.PN.&OS=PN/9070088&RS=PN/9070088.
[27] *Id.*
[28] *Id.*
[29] Complaint and Request for Investigation, Injunction, and Other Relief, *In re HireVue* (Nov. 6, 2019), https://epic.org/privacy/ftc/hirevue/EPIC_FTC_HireVue_Complaint.pdf.
[30] *See, e.g.*, Douglas Perry, *Emotion-recognition technologydoesn't work, but hiring professionals, others are using it anyway: report*, Oregonian (Dec. 16, 2019) https://www.oregonlive.com/business/2019/12/emotion-recognition-technology-doesnt-work-but-hiring-professionals-others-are-using-it-anyway-report.html; Algorithms in the Criminal Justice System, EPIC, https://epic.org/algorithmic-transparency/crim-justice/;
[31] Inception Impact Statement at 2.

EPIC recommends that the Commission adopts Option 3, subsection c.

EPIC recommends that the Commission adopt Option 3. In particular, the Commission should adopt subsections b and c, which would provide more protection for the public than subsection a. The risk in delineating between "high-risk" and other uses of AI is that information collected, maintained, or processed for one purpose may later be used for a different, unrelated purpose. For example, the United Kingdom recently signed McKinsey & Company to a contract for COVID-19 consulting services that would allow McKinsey to manage, disclose, and repurpose sensitive personal data about individuals for seven years after the purpose of the contract is fulfilled.[32] Last month, it was revealed the U.S. Secret Service purchases phone location data from private brokers that harvest data from apps that individuals are already using.[33]

If the Commission nevertheless chooses to define and regulate "high-risk" programs exclusively or differently, it should designate as "high-risk" all programs that impact people of different classes unequally, that invade personal privacy, or that lack adequate data security. The use of AI in the criminal justice system, the use of AI for secret consumer scoring, and the use of AI in hiring and educational settings all pose especially high risks.

As illustrated by the examples above, though, entities that collect data for one purpose often repurpose, synthesize, sell, or are compelled to turn over both the underlying data and the products of their AI synthesis of that data. Information collected under one purpose not previously determined as "high-risk" can easily be used in a "high-risk" purpose. Protecting consumers against all AI would ensure that complementary legislation will not be needed immediately, and that the intent of the regulations are carried out.

Both private and public uses of AI can threaten fundamental rights. Biases and other inaccuracies caused by AI systems can have a severely harmful impact on individuals, and enacting transparency and oversight requirements that applies to all AI systems is a critical step to help people understand and attempt to allay those harms.

Conclusion

The European Commission should enact strong regulations for all AI in order to protect fundamental rights. Oversight of both public and private uses of AI will help avoid inappropriate applications of the technology, minimize the opacity of AI decision-making, and avoid arbitrary actions and determinations. Specific mandatory obligations and oversight, as a part of Option 3 outlined in the Inception Impact Statement, would best achieve this goal.

Respectfully Submitted,

---

[32] Beckie Smith, *McKinsey banks 560,000 consulting on "vision, purpose and narrative" for new test and trace body*, Civil Service World (Aug. 18, 2020) https://www.civilserviceworld.com/news/article/mckinsey-banks-560000-consulting-on-vision-purpose-and-narrative-for-new-test-and-trace-body.

[33] See Joseph Cox, *Secret Service Bought Phone Location Data from Apps, Contract Confirms*, VICE (Aug. 17, 2020) https://www.vice.com/en_us/article/jgxk3g/secret-service-phone-location-data-babel-street.

Ben Winters
Ben Winters
EPIC Equal Justice Works Fellow

Sara Geoghegan
Sara Geoghegan
EPIC Consumer Protection Fellow