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

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

EUROPEAN COMMISSION FUNDAMENTAL RIGHTS POLICY UNIT

Request for Feedback in Parallel with the White Paper on Fundamental Rights

May 29, 2020

EPIC submits responses to the European Commission's request for comments in response to the following questions:

- Which situations [with the use of AI applications] do you view as high-risk situations from a fundamental rights perspective?
- How would you define high-risk situations in this regard?
- Do you know of effective means to address the risks that you identified in your reply to the above questions?
- Which single actors or groups of actors are best placed to address the risks that you identify?

EPIC is a public interest research center in Washington, D.C. that was established in 1994 to focus public attention on emerging privacy and related human rights issues, and to protect privacy, the First Amendment, and constitutional values.[1] EPIC has a long history of promoting transparency and accountability for information technology.[2]

EPIC has a particular interest in promoting algorithmic transparency and has consistently advocated for transparency and oversight through validation studies, reporting, and the application of the Universal Guidelines for AI ("UGAI") to promote trustworthy algorithms.[3] EPIC has pushed for

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

[2] 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/; 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.

[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-

transparency and accountability in the United States, and has litigated cases against the U.S. Department of Justice to compel production of documents regarding "evidence-based risk assessment tools"[4] and against the U.S. Department of Homeland Security to produce documents about a program to assess the probability that an individual commits a crime.[5] In 2018, EPIC and leading scientific societies petitioned the U.S. Office of Science and Technology Policy to solicit public input on U.S. Artificial Intelligence Policy.[6] EPIC submitted comments urging the National Science Foundation to adopt the UGAI, and to promote and enforce the UGAI across funding, research, and deployment of US AI systems.[7]

In an effort to establish necessary consumer safeguards, EPIC recently filed FTC complaints against HireVue,[8] an employment screening company, and AirBnB,[9] the rental service that claims to assess risk in potential renters based on an opaque algorithm. EPIC has also filed a petition with the FTC for a rulemaking for AI in Commerce.[10] EPIC recently published the *AI Policy Sourcebook*, the first reference book on AI policy.[11]

There are many AI principles set forth by industry, academia, civil society and governments. EPIC provides specific answers to the questions posed by the Commission below, but would like to also provide copies of the Universal Guidelines for Artificial Intelligence and the OECD AI Principles in their entirety, which EPIC supports as the baseline for AI regulation.

The Universal Guidelines for Artificial Intelligence ("UGAI"), 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:

1. Right to Transparency.
2. Right to Human Determination.

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) 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.* and 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.*

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]

Which situations [with the use of AI applications] do you view as high-risk situations from a fundamental rights perspective? How would you define high-risk situations in this regard?

High-risk programs include those that impact people of different classes unequally, that invade personal privacy, or lack adequate data security. In particular, 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 pose especially high risks.

Both private and public use of AI can lead to high-risk situations that threaten fundamental rights. Biases and other inaccuracies caused by AI systems deployed in these high-risk situations can have a severe impact on individuals.

Throughout the criminal justice system, the use of AI carries a high-risk of violating fundamental rights. The use of predictive algorithms in policing, facial recognition, drones, and the use of other AI systems in the law enforcement context create acute risks. There is an inherent tendency to perpetuate policing patterns that may already disproportionately disadvantage minorities. In pretrial dispositions, sentencing, and prisons, the use of algorithms to determine risk increases the likelihood that inaccurate, biased, or other improper results will exacerbate existing

[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.

inequalities.[18] 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 individual than for a white individual.[19] Specifically, NIST found "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."[20] 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.[21] 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 Congress as convicted criminals.[22]

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[23] (or in the words of Trooly's patent, to "determin[e] trustworthiness and compatibility of a person").[24] 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.[25] 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.[26] The company claims that the system can also identify "badness, anti-social tendencies, goodness, conscientiousness, openness, extraversion,

[18] *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.

[19] *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.

[20] *Id*.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] *Id.*

[26] *Id.*

agreeableness, neuroticism, narcissism, Machiavellianism, [and] psychopathy." AI systems such as HireVue that purport to detect subjective qualities for job applicants[27] is another risky form of consumer scoring. The accuracy of systems like this are suspect, and the AI is unaccountable and opaque. Furthermore, many of the "results" that these AI systems are designed to identify are highly subjective traits; there is no evidence that these subjective 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 these subjective, opaque, and potentially inaccurate systems. These systems accordingly present a high risk to fundamental rights.

Do you know of effective means to address the risks that you identified in your reply to the above questions?

Effective means to address risks like those identified above would include the following for high-risk functions of AI:

- Requiring independent, localized, and regular validation studies that include an analysis of racial, ethnic, and gender impacts for AI use by government.
- Requiring notification and consent of collection of data to be used in AI.
- Establish minimum technical security standards (e.g. encryption) and data governance (e.g. strong minimization, deletion, and retention policies) for any databases held and AI tools used.
- Publish key government uses of AI, including stated purposes, benefits and risks, costs and evaluations of efficacy.
- Make transparent the institutions responsible for every AI system and inform individuals when they are engaging with or being affected by an AI system.[28]
- Promote and support public development of AI systems that embrace international AI standards, including the EU standards, OECD standards, and the UGAI.
- For government utilization of technologies, require transparency, minimum technical security and data governance standards for any contractor.
- For violations of regulations, allow both consumer protection bodies as well as aggrieved individuals to bring causes of action.

Which single actors or groups of actors are best placed to address the risks that you identify?

The best group of actors to address identified risk are regulatory and legislative bodies. Optional adoption, or self-regulation, among developers is not a reliable method. The proliferation of ethics guidelines makes uniform self-regulation unlikely. Governments must implement policies that are reflective of the guidelines expressed in the Commission's White Paper and protective of fundamental rights. Governments can best understand, mitigate, and prevent through procurement reform, contract decisions, and strong laws establishing minimum requirements for AI deployment that affects fundamental rights.

[27] 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.

[28] *Universal Guidelines*, *supra* note 12, at 3, 10; *OECD AI Principles*, *supra* note 15, at 1.3.ii.

Conclusion

The European Commission should introduce strong regulations to ensure AI transparency and accountability. Oversight principles for government use of AI will help avoid inappropriate applications of the technology, minimize the opacity of public decision-making and avoid arbitrary government action. For private uses, legislation and regulation can establish a baseline standard for AI through the aforementioned requirements and associated threats of penalty. The lines separating government and corporate uses of AI are becoming increasingly blurred, particularly for law enforcement applications, which necessitates uniform rules across public and private sectors.

There is broad consensus internationally that AI systems should be regulated. Civil society, governments, inter-governmental organizations, and the private sector have all published principles for ethical and rights-based approaches to AI.[29] This consensus indicates widespread recognition of the need to regulate AI proactively and meaningfully.

Respectfully Submitted,

Ben Winters
Ben Winters
EPIC Equal Justice Works Fellow

[29] *Rome Call for AI Ethics*, The Vatican (Feb. 28th, 2020) http://www.academyforlife.va/content/dam/pav/documenti%20pdf/2020/CALL%2028%20febbraio/AI%20Rome%20Call%20x%20firma_DEF_DEF_.pdf.