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

PATENT AND TRADEMARK OFFICE

Intellectual Property Protection for Artificial Intelligence Innovation

84 CFR 66176

January 10, 2020

Published on October 30, 2019, the United States Patent and Trademark Office within the Department of Commerce ("USPTO") requests comments on Intellectual Property Protection for Artificial Intelligence Innovation.[1]

The agency seeks comments on the "copyright, trademark, and other intellectual property rights issues that may be impacted by AI."[2] EPIC submits these comments to the USPTO to (1) draw attention to the US endorsement of the OECD AI Principles; (2) to recommend that transparency, accountability, and human determination guide US AI policymaking; and (3) to recommend limiting the scope of Trade Secret defenses for risk assessment tools and other AI that has a legal or significant effect on an individual.

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.[3] EPIC has a particular interest in promoting

---

[1] Dep't of Commerce, *Request for Comments on Intellectual Property Protection for Artificial Intelligence Innovation*, 84 Fed.Reg. 58141 (October 30, 2019), https://www.govinfo.gov/content/pkg/FR-2019-10-30/pdf/2019-23638.pdf.
[2] *Id* at 58141.
[3] EPIC, *About EPIC* (2019), https://epic.org/epic/about.html.

algorithmic transparency and has consistently advocated for the release of reports, validation studies, and use of the Universal Guidelines for AI to guide requirements for trustworthy algorithms.[4] As EPIC President Marc Rotenberg has explained, "Algorithmic accountability is a complex topic, but the impact cuts broadly across life in America, from jobs and credit to housing and criminal justice."[5] EPIC has litigated cases against the Department of Justice to compel production of documents regarding "evidence-based risk assessment tools"[6] and the Department of Homeland Security to produce documents about a program to assess the probability that an individual commits a crime.[7] EPIC has also recently published the second edition of the *AI Policy Sourcebook*, the first reference book on AI policy.[8]

(1) US Endorsement of OECD AI Principles, OSTP/OMB Guidance for Regulation of AI Applications

The United States government has taken official steps to guide AI policy in the United States, which the USPTO's regulation is obligated to reflect. First, the United States is a signatory to the Organization for Economic Co-Operation and Development's Principles on Artificial Intelligence ("OECD AI Principles"), adopted in May 2019 by 42 member countries.[9] The third of five OECD AI Principles is that AI systems should have "transparency and responsible disclosure…to ensure that people understand AI-based outcomes and can challenge them." The other OECD principles state that "AI should benefit people"; should be "designed in a way that respects the rule of law, human rights, democratic values and diversity, and they should include appropriate safeguard"; "must

[4] *See* e.g. EPIC v. DOJ (D.C. Cir.) (18-5307), EPIC v CPB, EPIC v. DHS, FOIA requests, https://epic.org/foia/doj/criminal-justice-algorithms/.
[5] Marc Rotenberg, Editorial, *Bias by Computer*, N.Y. Times, Aug. 11, 2016, at A22, https://www.nytimes.com/2016/08/11/opinion/bias-by-computer.html.
[6] EPIC, *EPIC v. DOJ (Criminal Justice Algorithms)* https://epic.org/foia/doj/criminal-justice-algorithms/.
[7] *See Id.* and EPIC, *EPIC v. DHS (FAST Program)* https://epic.org/foia/dhs/fast/.
[8] *EPIC AI Policy Sourcebook 2020* (EPIC 2020),https://epic.org/bookstore/ai2020/.
[9] Organisation for Economic Co-operation and Development, *OECD Principles on AI* (May 2019) https://www.oecd.org/going-digital/ai/principles/.

function in a robust secure, and safe way throughout their life cycles"; and that accountability for those "developing, deploying or operating AI" is imperative.

Second, in January 2020, the White House Office of Science and Technology Policy ("OSTP") along with Office of Management and Budget ("OMB") published a memorandum[10] that instructs federal agencies to incorporate ten key principles when regulating Artificial Intelligence. Among these are Public Trust in AI; Public Participation; Scientific Integrity; Fairness and Non-Discrimination; Disclosure and Transparency; and Safety and Security. In the OSTP/OMB memorandum, transparency and public participation are repeatedly emphasized. In announcing the Guidance for Regulation of Artificial Intelligence Applications, US Chief Technology Officer Michael Kratsios said "The White House calls on agencies to protect privacy and promote civil rights, civil liberties, and American values in the regulatory approach to AI. Among other important steps, agencies should examine whether the outcomes and decisions of an AI application could result in unlawful discrimination, consider appropriate measures to disclose when AI is in use, and consider what controls are needed to ensure the confidentiality and integrity of the information processed, stored and transmitted in an AI system."[11] The USPTO should abide by the tenets set out in the OSTP/OMB Guidance for Regulation of Artificial Intelligence Applications.

(2) Universal Guidelines for AI

EPIC further recommends that USPTO incorporate the guidelines for AI policymaking expressed in the Universal Guidelines for AI ("UGAI"). The UGAI establishes principles to govern automated decision-making, and have been endorsed by over 250 individuals and 64 organizations

[10] Russel T. Vought, *Memorandum for the Heads of Executive Departments and Agencies: Guidance for Regulation of Artificial Intelligence Applications*, Office of Management and Budget (Jan. 7, 2020) https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf.

[11] Michael Kratsios, *AI That Reflects American Values*, Bloomberg (Jan. 7, 2020) https://www.bloomberg.com/opinion/articles/2020-01-07/ai-that-reflects-american-values?srnd=opinion.

worldwide. The first principle holds that "All individuals have the right to know the basis of an AI decision that concerns them. This includes access to the factors, the logic, and techniques that produced the outcome."[12]

3) Algorithmic Accountability and Trade Secrecy

It is important that transparency and algorithmic accountability are prioritized, especially when an AI system has a significant impact on the subject's life. Presently, individuals impacted by AI are unable to assess whether determinations were fair, accurate, transparent, replicable, and provable. Partially automated decisions also inform important decisions about people's lives but there is no legal right in the U.S. to human review of a fully automated decision.[13] A Pew Research Center study shows that a "majority of Americans find it unacceptable to use algorithms to make decisions with real-world consequences for humans."[14] Among the types of algorithms that were asked in that study were about the use of algorithms in resume screening, job interviews, personal finance scores, and criminal risk assessment for people up for parole.[15] These algorithms remain largely opaque in part because of a robust trade secret defense system for the developers.

Companies use trade secret law as a broad defense to transparency in the context of automated actuarial risk assessment algorithms utilized by courts throughout the country. Pre-trial risk assessments are algorithms aimed to assist judges, to varying degrees, in determining likelihood of re-offense as well as the likelihood that they will fail to appear at trial. Other AI assessment tools calculate risk and inform decisions about parole, policing, and prison management. Trade secrets

---

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

[13] A bill introduced in the House of Representatives would create this right. Online Privacy Act, 116th Congress, 1st Session https://eshoo.house.gov/wp-content/uploads/2019/11/Bill-Text-Online-Privacy-Act-Eshoo-Lofgren.pdf

[14] Aaron Smith, *Public Attitudes Toward Computer Algorithms*, (Nov. 16, 2018) https://www.pewresearch.org/internet/2018/11/16/public-attitudes-toward-computer-algorithms/.

[15] *Id*.

commonly act as broad defenses to Freedom of Information requests[16] about these tools as well as in court when defendants request production of documents.[17]

States increasingly recognize that trade secret claims must not diminish fairness or transparency in a decision that significantly impacts a person's life. The Idaho legislature passed a law in 2019 which provides that "a party to a criminal case wherein a court has considered, or an expert witness has relied upon, a pretrial risk assessment tool shall be entitled to review all calculations and data used to calculate his own risk score;" which specifies particularly that "no builder or user of a 'pretrial risk assessment tool' may assert trade secret or other protections in order to quash discovery in a criminal or civil case."[18] Further, at least four states have passed laws that create commissions or task forces to organize the different ways their state uses AI and recommend legislation, with transparency as a chief concern.[19] Although the impacts of these laws have not yet been fully realized, the need for transparency as a result of bias and accuracy concerns in these tools has been legislatively recognized. Studies have revealed bias or disparate impact of the use of these systems based on race, gender, and ethnicity among others.[20] And the risk of bias isn't limited to risk assessments. A study from the National Institute of Standards and Technology ("NIST") analyzed

---

[16] See, e.g. Andrea' R. Barnes, Mississippi Department of Corrections Response to EPIC FOIA request (Dec. 5, 2019) http://epic.org/EPIC-19-11-25-2019-FOIA-20191203-Agency-Response-Trade-Secret-Delay.pdf.
[17] See *Loomis v. Wisconsin*, 881 N.W.2d 749 (Wis. 2016).
[18] Idaho Leg. 19-1910(1)(b)-(c).
[19] *See* NYC Local Law 49, Int No. 1696-A §1(b)(2) (2017) https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3137815&GUID=437A6A6D-62E1-47E2-9C42-461253F9C6D0; NY Senate 3971-B (February 22, 2019) https://www.nysenate.gov/legislation/bills/2019/s3971; VT. H. 378 (May 21, 2018) https://legislature.vermont.gov/bill/status/2018/H.378; AL. SJR71 (May 15, 2019) http://alisondb.legislature.state.al.us/ALISON/SearchableInstruments/2019RS/PrintFiles/SJR71-int.pdf.
[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) 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*, Washington University Law Review, Vol. 96, 2018; https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3225350; Julia Angwin, Jeff Larson, Surya Mattu, and Lauren Kirchner, *Machine Bias*, ProPublica (May 23, 2016) https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.w

the facial recognition algorithms of a "majority of the industry" and found the software up to 100 times more likely to return a false positive of a non-white individual than white individuals.[21] Specifically, NIST found "for one-to-many matching, the team saw higher rates of false positives for African American females," which they highlight "are particularly important because the consequences could include false accusations."[22] The USPTO has an opportunity to set a federal baseline of greater transparency to limit the use of technologies with clearly biased effects such as the facial recognition software programs studied by NIST. Limiting trade secret defenses will allow greater opportunity for research and accountability within these tools, as well as empower the subjects of the tools.

The USPTO should focus on two distinct aspects of transparency surrounding automated tools: (1) the existence and use cases of the AI systems, and (2) the logic and operation of the systems once their existence is known. The trade secret defenses exacerbate problems in both domains. Although the USPTO describes trade secrets as "a complement to patent protection,"[23] Professor Frank Pasquale explains that, "trade secrecy effectively creates a property right in many algorithms whose creators do not want to disclose in patent applications."[24]

The USPTO should limit the strength of trade secret protection for algorithms or other AI programs that have a legal or significant effect, borrowing the standard of consumer-focused General Data Protection Regulation. Article 22 of the General Data Protection Regulation holds that a person "shall have the right not to be subject to a decision based solely on automated processing, including

---

[21] *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software*, National Institute of Standards and Technology, December 19, 2019 https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.
[22] *Id*.
[23] Trade Secret Policy, United States Patent and Trademark Office https://www.uspto.gov/ip-policy/trade-secret-policy
[24] Frank Pasquale, *Restoring Transparency to Automated Authority*, 9 Journal on Telecommunications & High Technology Law 235 (2011). https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=2357&context=fac_pubs.

profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."[25]

Conclusion

EPIC recommends that the USPTO ensure compliance with the OECD AI Principles, the OSTP/OMB Guidance on Regulation of Artificial Intelligence Applications, and the Universal Guidelines for AI. EPIC specifically recommends that the USPTO limit the scope of Trade Secret defenses for risk assessment tools that has a legal or significant effect on an individual.

Respectfully submitted,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Ben Winters*
Ben Winters
EPIC Equal Justice Works Fellow

[25] Art 22. EU GDPR Section 1.