Before the
FEDERAL TRADE COMMISSION
Washington, D.C. 20580

In Re: Petition for Rulemaking Concerning Use of Artificial Intelligence in Commerce	Docket No. _________

PETITION FOR RULEMAKING

The Electronic Privacy Information Center ("EPIC") hereby respectfully petitions the Federal Trade Commission ("FTC") to conduct a trade regulation rulemaking under 15 U.S.C. § 57a concerning the use of artificial intelligence ("AI") in commerce. Though AI has the potential to advance science, medicine, commerce, and education, the unregulated use of AI techniques has already caused serious harm to consumers, who are increasingly subject to opaque and unprovable decision-making in employment, credit, healthcare, housing, and criminal justice. Moreover, the absence of effective regulation has accelerated the spread of unaccountable and untrustworthy AI tools with immediate impacts on American consumers. Given the scale of commercial AI use, the rapid pace of AI development, and the very real consequences of AI-enabled decision-making for consumers, the Commission should immediately initiate a rulemaking to define and prevent consumer harms resulting from AI. Chairman Simons, in announcing the FTC's recent series of public hearings on consumer protection,[1] warned that the rise of AI "challenge[s] all of us to reexamine our regulatory approaches."[2] And as

[1] *Hearings on Competition and Consumer Protection in the 21st Century*, Fed. Trade Comm'n (Sep. 13, 2019), https://www.ftc.gov/policy/hearings-competition-consumer-protection.
[2] Joseph Simons, Chairman, Fed. Trade Comm'n, Remarks of Chairman Joseph Simon at the Second Annual Privacy Shield Review (Oct. 18, 2018),

Commissioner Slaughter urged last month, "[I]t is imperative for the FTC to take all action within its authority right now to protect consumers in this space."[3]

INTEREST OF PETITIONER

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, DC. EPIC was established in 1994 to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age. EPIC has played a leading role in developing the authority of the FTC to address emerging privacy issues and to safeguard the privacy rights of consumers.[4]

EPIC is also a longstanding advocate of algorithmic transparency and legal safeguards for the use of artificial intelligence.[5] As we previously 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."[6] More recently, EPIC acknowledged that "[t]he White House has

https://www.ftc.gov/system/files/documents/public_statements/1416593/chairman_joe_simons_privacy_shield_review_remarks-2018.pdf.

[3] Rebecca Kelly Slaughter, Comm'r, Fed. Trade Comm'n, Algorithms and Economic Justice, Remarks of Commissioner Rebecca Kelly Slaughter at UCLA School of Law 15 (Jan. 24, 2020), https://www.ftc.gov/system/files/documents/public_statements/1564883/remarks_of_commissioner_rebecca_kelly_slaughter_on_algorithmic_and_economic_justice_01-24-2020.pdf.

[4] *See, e.g.*, Comments of EPIC, *In re Unrollme, Inc.,* FTC File No. 172 3139 (Sep. 19, 2019), https://epic.org/apa/comments/EPIC-FTC-Unrollme-Sept2019.pdf; Comments of EPIC, *In re Aleksandr Kogan and Alexander Nix*, FTC File No. 182 3106 & 182 3107 (Sep. 3, 2019), https://epic.org/apa/comments/EPIC-FTC-CambridgeAnalytica-Sept2019.pdf; Comments of EPIC, *Standards for Safeguarding Customer Information*, FTC Document No. 2019-10910 (Aug. 1, 2019), https://epic.org/apa/comments/EPIC-FTC-Safeguards-Aug2019.pdf; Complaint, Request for Investigation, Injunction, and Other Relief, *In re Zoom Video Commc'ns, Inc.* (July 11, 2019), https://epic.org/privacy/ftc/zoomEPIC-FTC-Complaint-In-re-Zoom-7-19.pdf; Comments of EPIC, *In re Uber Technologies, Inc.*, FTC File No. 152-3054 (May 14, 2018), https://epic.org/apa/comments/EPIC-FTC-Revised-Uber-Settlement.pdf; Comments of EPIC, *In re Paypal, Inc.*, FTC File No. 162-3102 (Mar. 29, 2018), https://epic.org/apa/comments/EPIC-FTC-PayPal-ConsentOrder.pdf; Complaint, Request for Investigation, Injunction, and Other Relief, *In re Google Inc.* (July 31, 2017), https://www.epic.org/privacy/ftc/google/EPIC-FTC-Google-Purchase-Tracking-Complaint.pdf; Complaint and Request for Investigation, Injunction, and Other Relief, *In re Genesis Toys and Nuance Communications* (Dec. 6, 2016), https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf.

[5] EPIC, *Algorithmic Transparency: End Secret Profiling* (2020), https://epic.org/algorithmic-transparency/.

[6] Marc Rotenberg, EPIC President, *Bias by Computer*, N.Y. Times (Aug. 10, 2016), https://www.nytimes.com/2016/08/11/opinion/bias-by-computer.html.

already made some progress on this front, highlighting American values, including privacy and civil liberties, in an executive order earlier this year, and backing an important international framework at the Organization for Economic Cooperation and Development."[7] But we also warned of the urgency to act now: "The United States must work with other democratic countries to establish red lines for certain A.I. applications and ensure fairness, accountability and transparency as A.I. systems are deployed."[8]

EPIC has specifically recommended that the FTC respond to the emergence of AI techniques that are "unfair or deceptive," and therefore in violation of the FTC Act.[9] In May 2017, EPIC filed a complaint with the Commission highlighting the use of a "secret, proprietary algorithm, used to assign personally identifiable numeric scores to tennis players under 13 years old and others, known as the Universal Tennis Rating ('UTR')."[10] EPIC explained that the UTR "collects a wide range of tennis-related information, including online data, to generate and assign ratings for all players in Universal Tennis's system" and that "[p]layers in nearly all organized U.S. and many international leagues are rated by this algorithm without the opportunity to opt out and without knowledge of the actual logic used to create the rating."[11] EPIC alleged that the use of this secret algorithm by Universal Tennis, LLC constituted an unfair and deceptive trade practice and violated the Children's Online Privacy Protection Act.[12]

In November 2019, EPIC filed a complaint with the Commission highlighting HireVue, Inc.'s use of proprietary AI to evaluate the qualifications of job candidates based largely on voice

[7] Marc Rotenberg, EPIC President, *The Battle Over Artificial Intelligence*, N.Y. Times (Apr. 19, 2019), https://www.nytimes.com/2019/04/18/opinion/letters/artificial-intelligence.html.
[8] *Id.*
[9] 15 U.S.C. § 45(a)(1).
[10] Complaint, Request for Investigation, Injunction, and Other Relief ¶ 1, *In re Universal Tennis, LLC* (May 17, 2017), https://epic.org/algorithmic-transparency/EPIC-FTC-UTR-Complaint.pdf.
[11] *Id.* ¶ 2.
[12] *Id.* ¶¶ 3–4.

and appearance.[13] EPIC explained that "HireVue's use of secret algorithms to analyze job candidates' biometric data violates widely-adopted ethical standards for the use of artificial intelligence,"[14] including the Organisation for Economic Co-operation and Development ("OECD") Principles on Artificial Intelligence[15] and the Universal Guidelines for Artificial Intelligence ("UGAI").[16] EPIC "urge[d] the Commission to investigate HireVue and to find that its uses of facial recognition technology, biometric data, and secret, unproven algorithms constitute unfair and deceptive trade practices[.]"[17]

BACKGROUND

A. Public policy frameworks require that AI systems be transparent, accountable, trustworthy, and fair.

Artificial intelligence poses unique risks to human rights, privacy, and autonomy. As Professors Danielle Keats Citron and Frank Pasquale explain, "New algorithmic decisionmakers are sovereign over important aspects of individual lives. If law and due process are absent from this field, we are essentially paving the way to a new feudal order of unaccountable reputational intermediaries."[18] Accordingly, policymakers and experts have established widely adopted legal standards for the use of AI.

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

[14] *Id.* ¶ 60.

[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; *see also* EPIC, *The AI Policy Sourcebook 2020* at 111–21 (Marc Rotenberg ed., 2020).

[16] *Universal Guidelines for Artificial Intelligence*, The Public Voice (Oct. 23, 2018) [hereinafter *Universal Guidelines*], https://thepublicvoice.org/ai-universal-guidelines/; *see also* EPIC, *The AI Policy Sourcebook 2020*, *supra* note 15, at 170–75.

[17] EPIC HireVue Complaint, *supra* note 13, ¶¶ 9–12.

[18] Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1, 19 (2014).

The OECD AI Principles[19] were adopted in 2019 and endorsed by 42 countries—including the United States and the G20 nations.[20] 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.[21]

The OECD AI Principle on Transparency and Explainability specifically states: "AI Actors should commit to transparency and responsible disclosure regarding AI systems. To this end, they should provide meaningful information, appropriate to the context, and consistent with the state of art: . . . to enable those adversely affected by an AI system to challenge its outcome based on plain and easy-to-understand information on the factors, and the logic that served as the basis for the prediction, recommendation or decision."[22] "AI Actors" are defined as those "who play an active role in the AI system lifecycle, including organisations and individuals that deploy or operate AI."[23]

The OECD also urges governments to ensure the development of "trustworthy AI" and to focus on "AI-related social, legal and ethical implications and policy issues."[24] Governments are specifically urged to "review and adapt, as appropriate, their policy and regulatory frameworks and assessment mechanisms as they apply to AI systems to encourage innovation and competition for trustworthy AI."[25]

[19] *OECD AI Principles*, *supra* note 15.

[20] *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.

[21] *OECD AI Principles*, *supra* note 15.

[22] *Id.* at 1.3.

[23] *Id.* at I.

[24] *OECD AI Principles*, *supra* note 15.

[25] *Id.* at 2.3(b).

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.[26] The Universal Guidelines for AI have been endorsed by more than 250 experts and 60 organizations in 40 countries.[27] The UGAI comprise twelve principles:

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.[28]

Among the key principles, the UGAI states: "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" (*Right to Transparency*); "Institutions must ensure that AI systems do not reflect unfair bias or make impermissible discriminatory decisions" (*Fairness Obligation*); "An AI system should be deployed only after an adequate evaluation of its purpose and objectives, its benefits, as well as its risks. Institutions must be responsible for decisions made by an AI system" (*Assessment and Accountability Obligation*); "Institutions must ensure the accuracy, reliability, and validity of decisions" (*Accuracy, Reliability, and Validity Obligations*); and "Institutions must establish data provenance, and assure quality and relevance for the data input into algorithms" (*Data Quality Obligation*).

[26] *Universal Guidelines*, *supra* note 16.

[27] *Universal Guidelines for Artificial Intelligence: Endorsement*, The Public Voice (2020), https://thepublicvoice.org/AI-universal-guidelines/endorsement/.

[28] *Universal Guidelines*, *supra* note 16.

Recently, the Council of Europe released its "Draft Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems."[29] The Recommendation would similarly impose requirements of transparency, accountability, identifiability, evaluation, and contestability on both public and private sector uses of AI. The draft recommendation of the Council of Europe states, for example:

> Affected individuals and groups should be afforded effective means to contest relevant determinations and decisions. As a necessary precondition, the existence, process, rationale, reasoning and possible outcome of algorithmic systems at individual and collective level should be explained and clarified in a timely, impartial, easily-readable and accessible manner to individuals whose rights or legitimate interests may be affected, as well as to relevant public authorities.[30]

Major scientific organizations—including the Association for Computing Machinery ("ACM") and the Institute of Electrical and Electronics Engineers ("IEEE")—have also issued guidelines on the use of AI.[31] The ACM guidelines warn that "algorithms and analytics can be opaque, making it impossible to determine when their outputs may be biased or erroneous,"[32] and the IEEE highlights the "need to establish societal and policy guidelines in order for such systems to remain human-centric, serving humanity's values and ethical principles."[33]

[29] Comm. of Experts MSI-AUT, Council of Europe, *Addressing the Impacts of Algorithms on Human Rights: Draft Recommendation of the Committee of Ministers to Member States on the Human Rights Impacts of Algorithmic Systems* (2018), https://rm.coe.int/draft-recommendation-of-the-committee-of-ministers-to-states-on-the-hu/168095eecf.

[30] *Id.* at 10.

[31] Assoc. for Comput. Mach., *Statement on Algorithmic Transparency and Accountability*, (Jan. 12, 2017), https://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_algorithms.pdf; Inst. of Elec. & Elec. Eng'rs, *Ethically Aligned Design* (2017), https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead1e.pdf; *see also* EPIC, *The AI Policy Sourcebook 2020*, *supra* note 15, at 144–46, 157–68.

[32] Assoc. for Comput. Mach., *supra* note 31, at 1.

[33] Inst. of Elec. & Elec. Eng'rs, *supra* note 31, at 2.

B. The OMB Guidance for Regulation of Artificial Intelligence Applications requires transparency, accountability, trustworthiness, and fairness in the use of AI.

In January 2020, the Office of Management and Budget, in coordination with the Office of Science and Technology and Policy, released its Guidance for Regulation of Artificial Intelligence Applications.[34] The OMB AI Guidance, which applies to "all Federal agencies," incorporates many of the precepts of the OECD AI Principles and the UGAI. The OMB AI Guidance lays out ten "Principles for the Stewardship of AI Applications":

1. Public Trust in AI.
2. Public Participation.
3. Scientific Integrity and Information Quality.
4. Risk Assessment and Management.
5. Benefits and Costs.
6. Flexibility.
7. Fairness and Non-Discrimination.
8. Disclosure and Transparency.
9. Safety and Security.
10. Interagency Coordination.[35]

The OMB Guidance for Regulation of AI warns that "AI applications could pose risks to privacy, individual rights, autonomy, and civil liberties that must be carefully assessed and appropriately addressed. Its continued adoption and acceptance will depend significantly on public trust and validation."[36] The OMB further instructs that "[w]hen considering regulations or policies related to AI applications, agencies should continue to promote advancements in technology and innovation, while protecting American technology, economic and national

[34] Russell T. Vought, Acting Dir., Office of Mgmt. & Budget, *Memorandum for the Heads of Executive Departments and Agencies: Guidance for Regulation of Artificial Intelligence Applications* (Jan. 7, 2020), https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf.
[35] *Id.* at 3–6.
[36] *Id.* at 3.

security, privacy, civil liberties, and other American values, including the principles of freedom, human rights, the rule of law, and respect for intellectual property."[37]

At the time of the release of the OMB Guidance for Regulation of AI, U.S. Chief Technology Officer Michael Kratsios wrote:

> 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."[38]

C. Businesses are currently relying on opaque AI techniques to make life-altering decisions about consumers.

Common to the OECD AI Principles, the UGAI, and the OMB AI Guidance is the requirement that AI be transparent and explainable. Yet businesses routinely violate this principle by relying on opaque decision-making tools to make life-altering decisions about consumers in housing, employment, education, credit, and commerce. As Professors Citron and Pasquale have explained, "though automated scoring is pervasive and consequential, it is also opaque and lacking oversight."[39]

One prominent example is HireVue, Inc., a service that uses proprietary AI to evaluate the qualifications of job candidates based largely on voice and appearance. EPIC previously filed an FTC complaint highlighting the unfairness of HireVue's screening practices.[40] When a job candidate seeks employment at a company that uses HireVue's algorithmic assessment services,

[37] *Id.* at 1.
[38] 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.
[39] Citron & Pasquale, *supra* note 18, at 1.
[40] EPIC HireVue Complaint, *supra* note 13.

HireVue administers an online “video interview” and/or an online “game-based challenge[]” to the candidate.[41] HireVue collects “tens of thousands of data points”[42] from each video interview and a “rich and complex” array of data from each “psychometric game[.]”[43] HireVue then inputs these personal data points into “predictive algorithms”[44] that allegedly determine each job candidate’s “employability,” “cognitive ability,” “psychological traits,” “emotional intelligence,” and “social aptitudes.”[45] But HireVue does not give candidates access to the training data, factors, logic, or techniques used to generate each algorithmic assessment. In some cases, even HireVue is unaware of the basis for an assessment.[46]

As EPIC has determined, the scope of AI use in employment screening is sweeping. HireVue—just one competitor in the employment screening field—has over 700 corporate customers, including major companies like Hilton, Ikea, Oracle, Dow Jones, Koch Industries, Unilever, Urban Outfitters, Carnival, Under Armour, Vodafone, Dunkin’ Brands, Keurig Dr Pepper, Cathay Pacific, AB InBev, HBO, Sequoia, Staples, BASF, CARFAX, CDW, Conoco Phillips, Panda Express, Penguin Random House, and Anheuser-Busch.[47] Nonprofits and public sector employers also use HireVue’s assessment services, including Atlanta Public Schools and Thurgood Marshall College Fund.[48] Talview Inc., a competitor to HireVue, offers a similar suite of AI-powered resume scanning, “AI video interviews with behavioral insights,” and “[o]nline

[41] *Id.*
[42] *How to Prepare for Your HireVue Assessment* HireVue (Apr. 16, 2019), https://www.hirevue.com/blog/how-to-prepare-for-your-hirevue-assessment; Nathan Mondragon et al., HireVue, *The Next Generation of Assessments* 6 (Feb. 2019).
[43] Mondragon et al., *supra* note 42*,* at 5.
[44] *Id.* at 7.
[45] HireVue, *supra* note 42; Mondragon et al., *supra* note 42 at 6.
[46] Drew Harwell, *A face-scanning algorithm increasingly decides whether you deserve the job*, Wash. Post (Oct. 25, 2019), https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/.
[47] *Customers*, HireVue (2019), https://www.hirevue.com/customers.
[48] *Id.*

assessments."[49] And Affectiva, Inc. "analyzes human states in context," using "computer vision, speech analytics, deep learning and a lot of data."[50] Yet the algorithms used to make these determinations are kept secret from the consumers under evaluation.

Nor, as EPIC has determined, is the use of opaque AI tools limited to the employment context. Students are subject to AI-based analysis, including automated screening of their communications on school-mandated laptops.[51] Individuals are pressed to hand over intimate, real-time health data to insurance giants—data which may be fed into undisclosed risk assessment tools.[52] And DNA testing services GEDmatch and 23andMe rely on proprietary algorithms to develop genetic profiles of consumers, information which law enforcement routinely seeks to obtain and use.[53] More and more, consumers are subjected to AI decision-making yet prevented from learning the grounds on which those decisions are made.

C. Businesses are employing AI with little or no accountability to consumers.

The OECD AI Principles dictate that "organisations and individuals developing, deploying or operating AI systems should be held accountable for their proper functioning"[54]—a requirement that is also set out in the UGAI and established in the OMB Guidance for Regulation of AI. Yet businesses routinely subject consumers to AI decision-making and scoring with little or no accountability. "Although some scores, such as credit, are available to the public, the scorers refuse to reveal the method and logic of their predictive systems. No one can

[49] Talview (2020), https://www.talview.com/.

[50] Affectiva (2020), https://www.affectiva.com/.

[51] Charlie Warzel, *Welcome to the K-12 Surveillance State*, N.Y. Times (Jul. 2, 2019) https://www.nytimes.com/2019/07/02/opinion/surveillance-state-schools.html.

[52] Stephanie O'Neill, *As Insurers Offer Discounts For Fitness Trackers, Wearers Should Step With Caution*, NPR (Nov. 19, 2018), https://www.npr.org/sections/health-shots/2018/11/19/668266197/as-insurers-offer-discounts-for-fitness-trackers-wearers-should-step-with-cautio.

[53] Elizabeth Joh, *Want to See My Genes? Get a Warrant*, N.Y. Times (Jun. 11, 2019).

[54] *OECD AI Principles*, *supra* note 15, at 1.5.

challenge the process of scoring and the results because the algorithms are zealously guarded trade secrets."[55]

One of the most alarming examples of this, Clearview AI, came to light just weeks ago.[56] Using a powerful algorithm and billions of facial images collected without consent, Clearview has deployed a facial recognition app capable of quickly identifying a person based on a single photo.[57] By the time the public was made aware of Clearview's existence, the app was already in use by hundreds of law enforcement agencies.[58] Clearview built its tool in effective secrecy, in violation of numerous terms of service, and with no oversight. Yet despite the recent public outcry over Clearview's use of AI, individual consumers have little ability to hold the company accountable for developing and operating a facial recognition tool based on their personal data. And Clearview is not alone in the field: companies including Amazon,[59] FaceFirst,[60] and Vigilant Solutions[61] have also developed large-scale—and largely unaccountable—facial recognition tools.

D. Businesses have failed to ensure that AI is fair to consumers and free from impermissible bias.

Fairness is one of the cornerstones of AI use. As established in the OECD AI Principles, "AI systems should be designed in a way that respects the rule of law, human rights, democratic values and diversity, and they should include appropriate safeguard—for example, enabling human intervention where necessary—to ensure a fair and just society."[62] The UGAI emphasizes

[55] Citron & Pasquale, *supra* note 18, at 5.

[56] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. Times (Jan. 18, 2020) https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[57] *Id.*

[58] *Id.*

[59] *Amazon Rekognition*, AWS (2020), https://aws.amazon.com/rekognition/.

[60] FaceFirst (2020), https://www.facefirst.com/.

[61] *Vigilant FaceSearch*, Vigilant Solutions (2020), https://www.vigilantsolutions.com/products/facial-recognition/.

[62] *OECD AI Principles*, *supra* note 15, at 1.2

that public safety must be also be considered: “Institutions must assess the public safety risks that arise from the deployment of AI systems that direct or control physical devices, and implement safety controls.” Yet time and again, businesses have failed to demonstrate that their use of AI is fair to consumers or free from impermissible bias. As Professors Citron and Pasquale again explain, “Although algorithmic predictions harm individuals' life opportunities often in arbitrary and discriminatory ways, they remain secret. Human oversight is needed to police these problems.”[63]

Last year, the National Institute of Standards and Technology (“NIST”) analyzed 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 for a non-white individual than for a white individual.[64] 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.”[65] 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.[66] A review of Rekognition—an Amazon-owned facial recognition company marketed to law enforcement—revealed indications of racial bias and found that the system misidentified 28 members of Congress as convicted criminals.[67] And still other studies have revealed racial,

[63] Citron & Pasquale, *supra* note 18, at 7–8.

[64] *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.

[65] *Id*.

[66] 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.

[67] 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.

ethnic, and gender bias in privately developed risk assessment tools used by governments to evaluate parolees and prisoners.[68]

E. Businesses are engaged in secret profiling of consumers.

The OECD AI Principles and the UGAI strictly prohibit secret profiling. The UGAI state that "[n]o institution shall establish or maintain a secret profiling system" and that "[t]he institution responsible for an AI system must be made known to the public."[69] Similarly, the OECD AI Principles emphasize that individuals be "aware of their interactions with AI systems."[70] Yet consumer profiling has become "pervasive, secret, and automated," posing "threats to human dignity[.]"[71] "At the very least, individuals should have a meaningful form of notice and a chance to challenge predictive scores that harm their ability to obtain credit, jobs, housing, and other important opportunities."[72]

Clearview AI and the Universal Tennis Rating are notable examples of secret profiling of consumers. But there are many others. In 2017, Airbnb acquired Trooly, an AI risk assessment tool that can be used to rate potential guests[73] (or in the words of Trooly's patent, to "determin[e] trustworthiness and compatibility of a person").[74] The AI system analyzes information collected

[68] *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.

[69] *Universal Guidelines*, *supra* note 16, at 3, 10.

[70] *OECD AI Principles*, *supra* note 15, at 1.3.ii.

[71] Citron & Pasquale, *supra* note 18, at 27.

[72] *Id.*

[73] 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.

[74] 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.

from third parties—including service providers, blogs, public and commercial databases, and social networks—to generate a “trustworthiness” score.[75] The patent 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.[76] According to the patent, the system can also identify “badness, anti-social tendencies, goodness, conscientiousness, openness, extraversion, agreeableness, neuroticism, narcissism, Machiavellianism, [and] psychopathy.” Yet whether and how Airbnb is using each of Trooly’s capabilities to screen consumers remains a secret.[77]

LEGAL BASIS FOR INITIATING A RULEMAKING

Given the increasing commercial use of opaque, unaccountable, unfair, and secret AI tools, it is imperative that the Commission conduct a rulemaking under 15 U.S.C. § 57a to protect consumers and establish a regulatory framework for AI.

Under the FTC Act, the Commission is empowered to issue trade regulation rules “which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce[.]”[78] These rules “may include requirements prescribed for the purpose of preventing such acts or practices.”[79] A violation of a trade rule “shall constitute an unfair or deceptive act or practice in violation of section 5(a)(1) of [the FTC] Act, unless the Commission otherwise expressly provides in its rule.”[80]

[75] *Id.*
[76] *Id.*
[77] Aaron Holmes, *Airbnb has patented software that digs through social media to root out people who display ‘narcissism or psychopathy’*, Business Insider (Jan. 6, 2020), https://www.businessinsider.com/airbnb-software-predicts-if-guests-are-psychopaths-patent-2020-1
[78] 15 U.S.C. § 57a(a)(1)(B).
[79] *Id.*
[80] 16 C.F.R. § 1.8(a).

The Commission may initiate a trade regulation rulemaking when "it has reason to believe that the unfair or deceptive acts or practices which are the subject of the proposed rulemaking are prevalent."[81] Acts or practices are "prevalent" if the Commission "has issued cease and desist orders regarding such acts or practices" or—as in this case—when "information available to the Commission indicates a widespread pattern of unfair or deceptive acts or practices."[82] Thus, the Commission may initiate a trade rulemaking upon learning of a "widespread pattern"[83] of unfair trade practices—that is, practices which "cause[] or [are] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[84]

As set forth above, businesses are using AI for a wide range of applications that directly affect and injure consumers. The injuries suffered by consumers are substantial: many commercial applications of AI implicate highly sensitive personal data, impose real-world consequences on consumers, and are difficult or impossible to avoid. Finally, these injuries are not outweighed by countervailing benefits. Accordingly, the Commission should immediately initiate a rulemaking to require accountability, transparency, and fairness in the use of artificial intelligence.

A. The use of many commercial AI tools is unfair to consumers.

The unregulated use of AI to make decisions about consumers is unfair because it "causes or is likely to cause substantial injury to consumers" that is not outweighed by countervailing benefits.[85] As explained by a former director of the Bureau of Consumer Protection: an injury

[81] 15 U.S.C. § 57a(b)(3).
[82] 15 U.S.C. § 57a(b)(3)(A)–(B).
[83] 15 U.S.C. § 57a(b)(3) B).
[84] 15 U.S.C. § 45(n).
[85] 15 U.S.C. § 45(n).

meets the "modern unfairness" standard if it is "(1) substantial, (2) without offsetting benefits, and (3) one that consumers cannot reasonably avoid[.]"[86] The Commission is expected to consider "established public policies" when determining whether trade practices are unfair.[87]

The injuries caused to consumers by commercial AI use are substantial and frequently unavoidable. In assessing privacy-related injuries to consumers, the Commission typically focuses on the sensitivity of the personal data at issue, the relationship between the consumer and the business(es) engaged in the challenged practice, and the consumers' knowledge of and agency over the practice.[88] These factors underscore the gravity of the injuries that consumers have suffered, and will continue to suffer, from the commercial deployment of AI. Businesses are regularly relying on biometric information, financial records, and other highly sensitive personal data to make individualized AI-based determinations about consumers. Many of these AI applications are completely unknown to consumers, as in the secret collection and processing of billions of facial images by Clearview. And even if consumers are notified that an AI system is in use, they are frequently given no explanation of the decisions made by that system and no meaningful opportunity to opt out. For example, many job applicants have little choice but to submit to HireVue's AI-based screening tool—or else forgo an ever-growing list of employment opportunities.

Moreover, commercial uses of AI routinely violate established public policy frameworks. As noted, the AI tools deployed by HireVue, Clearview, Airbnb, and numerous other corporations flout the U.S.-endorsed OECD AI Principles and the Universal Guidelines on

[86] J. Howard Beales, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, The Marketing and Public Policy Conference (May 30, 2003).
[87] 15 U.S.C. § 45(n).
[88] Cobun Keegan & Calli Schroeder, *Unpacking Unfairness: The FTC's Evolving Measures of Privacy Harms*, 15 J.L. Econ. & Pol'y 19, 32 (2019).

Artificial Intelligence. Instead, these AI tools are often opaque, unaccountable, and unreliable. For these reasons, strong majorities of the public have concluded that automated decisionmaking is "unacceptable" in criminal risk assessment (56%), resume screening (57%), job interviews (67%), and consumer scoring (68%).[89]

Finally, these consumer injuries are not offset by the benefits of the offending AI tools. Indeed, businesses frequently fail to demonstrate that AI decision-making tools are accurate, reliable, or necessary—if businesses even disclose the existence of these tools to consumers in the first place. For AI systems such as Clearview's facial recognition tool, such a showing would be impossible under any circumstances. Accordingly, a wide range of commercial uses of AI constitute "unfair" trade practices in violation of section 5 of the FTC Act.[90]

B. The widespread use of AI tools in commerce requires the Federal Trade Commission to exercise rulemaking authority.

Commercial applications of AI have become sufficiently widespread, or "prevalent,"[91] that the Commission must address the resulting unfairness to consumers through its trade regulation authority. The uses of AI described above—though extensive and alarming—are merely the tip of the iceberg. According to a Gartner study, the commercial use of AI has increased 270% in the last 4 years, with 37% of businesses now using some form of the technology.[92] By other accounts, the scale of commercial AI is even greater. Nearly half of respondents in one survey reported that "their organizations have embedded at least one [AI capability] into their standard business processes, while another 30 percent report piloting the use

[89] Aaron Smith, *7 things we've learned about computer algorithms*, Fact Tank, Pew Research Center (Feb. 13, 2019), https://www.pewresearch.org/fact-tank/2019/02/13/7-things-weve-learned-about-computer-algorithms/.
[90] 15 U.S.C. § 45.
[91] 15 U.S.C. § 57a(b)(3).
[92] *Gartner Survey Shows 37% of Organizations Have Implemented AI in Some Form*, Gartner (Jan. 21, 2019) https://www.gartner.com/en/newsroom/press-releases/2019-01-21-gartner-survey-shows-37-percent-of-organizations-have.

of AI."[93] And the National Academies of Medicine, NIST, and the Consumer Financial Protection Bureau have documented the growing role of AI in medicine, banking, and the defense sector.[94]

This Commission has repeatedly recognized that the rapid growth of AI implicates the FTC's regulatory powers. In October 2018, Chairman Simons explained that the rise of AI "challenge[s] all of us to reexamine our regulatory approaches."[95] The following month, the Commission hosted a public event on "Consumer Protection Implications of Algorithms, Artificial Intelligence, and Predictive Analytics."[96] Commissioner Wilson recently noted that the FTC "has long been thinking about and grappling with" issues of algorithmic bias and discrimination, [97] and Commissioner Phillips has acknowledged the FTC's power to "regulat[e] the private sector's use of technology and AI[.]"[98] Commissioner Chopra has repeatedly warned about the "opacity and complexity of algorithmic decision-making"[99] and that "we should never

[93] McKinsey Global Survey, *AI adoption advances, but foundational barriers remain* (Nov. 2018), https://www.mckinsey.com/featured-insights/artificial-intelligence/ai-adoption-advances-but-foundational-barriers-remain.

[94] Nat'l Acad. of Med., *Artificial Intelligence in Health Care: The Hope, The Hype, the Promise, the Peril* (Michael Matheny et al. eds., 2019), https://nam.edu/wp-content/uploads/2019/12/AI-in-Health-Care-PREPUB-FINAL.pdf; Nat'l Inst. of Sci. and Tech., *AI: Using Standards to Mitigate Risks* 7 (May 20, 2019), https://www.nist.gov/system/files/documents/2019/05/20/nist-ai-rfi-dhs-001.pdf; Consumer Fin. Prot. Bureau, *BCFP Collaborates With Regulators Around The World To Create Global Financial Innovation Network* (Aug. 7, 2018), https://www.consumerfinance.gov/about-us/newsroom/bcfp-collaborates-regulators-around-world-create-global-financial-innovation-network/.

[95] Joseph Simons, Chairman, Fed. Trade Comm'n, Remarks of Chairman Joseph Simon at the Second Annual Privacy Shield Review (Oct. 18, 2018), https://www.ftc.gov/system/files/documents/public_statements/1416593/chairman_joe_simons_privacy_shield_review_remarks-2018.pdf.

[96] *Consumer Protection Implications of Algorithms, Artificial Intelligence, and Predictive Analytics*, Fed. Trade Comm'n (Nov. 13, 2018), https://www.ftc.gov/news-events/audio-video/audio/consumer-protection-implications-algorithms-artificial-intelligence.

[97] Christine S. Wilson, Comm'r, Fed. Trade Comm'n, The Role of the Federal Trade Commission in Privacy and Beyond, Fireside Chat at the Brookings Institution (Oct. 28 2019), https://www.brookings.edu/wp-content/uploads/2019/10/gs_20191028_ftc_privacy_transcript.pdf.

[98] Sam Pfeifle, *FTC's Phillips Talks Regulating Tech Innovation*, IAPP (Oct. 26, 2018), https://iapp.org/news/a/ftcs-phillips-talks-regulating-tech-innovation/.

[99] Rohit Chopra, Comm'r, Fed. Trade Comm'n, Comment Letter on Proposed Rule to Amend HUD's Interpretation of the Fair Housing Act's Discriminatory Effects Standard 6 (Oct. 16, 2019),

assume that algorithms will be free of bias."[100] And last month, Commissioner Slaughter sounded the alarm about the "mounting and urgent" nature of "algorithmic harms," noting that a trade regulation rulemaking may be required:

> But the threats to consumers arising from data abuse, including those posed by algorithmic harms, are mounting and urgent. I think it is imperative for the FTC to take all action within its authority right now to protect consumers in this space. This authority includes our [Magnuson–Moss] rulemaking, which, although slow and imperfect, is available today and could generate a rule in this area if Congress ultimately fails to act. At the very least, initiating such a rulemaking would significantly advance the public debate through targeted study, thoughtful commentary, and nuanced proposals.
>
> In the area of algorithmic justice, a Mag-Moss rule might be able to affirmatively impose requirements of transparency, accountability, and remedy. A well-drafted rule could do so in a way that takes into account context and relative risk. This is not an easy endeavor, but it is a valuable one to consider.[101]

The concerns of the individual Commissioners are well-founded, and intervention by the Commission is urgently required.

Moreover, the rapidly escalating scale of unfair AI use makes it essential for the Commission to conduct a rulemaking rather than rely solely on case-by-case enforcement. By defining unfair and deceptive practices *ex ante*, and "with specificity,"[102] a trade regulation rule would "make it easier for the FTC to take action against" parties[103] that harm consumers through the use of AI. A rule on AI would also preclude arguments—like those raised by LabMD in

https://www.ftc.gov/system/files/documents/public_statements/1549212/chopra_-_letter_to_hud_on_disparate_impact_proposed_rulemaking_10-16-2019.pdf.

[100] Rohit Chopra, Comm'r, Fed. Trade Comm'n, Remarks of Federal Trade Commissioner Rohit Chopra at the Silicon Flatirons Conference 3 (Feb. 10, 2019), https://www.ftc.gov/system/files/documents/public_statements/1453633/remarks_of_commissioner_chopra_at_silicon_flatirons.pdf.

[101] Slaughter, *supra* note 3, at 15–16.

[102] 15 U.S.C. § 57a(a)(1)(B).

[103] Press Release, FTC Approves Final Amendments to its R-Value Rule for Home Insulation Products, Fed. Trade Comm'n (Oct. 28, 2018), https://www.ftc.gov/news-events/press-releases/2018/10/ftc-approves-final-amendments-its-r-value-rule-home-insulation.

response to the Commission's data security enforcement action—"that the Commission failed to provide fair notice"[104] concerning which practices are unfair and unlawful.

As we have warned, "the battle over the future of artificial intelligence will not simply be about who gathers the top scientists or who is first to innovate. It will also be about who is able to preserve fundamental rights during a period of rapidly changing technology."[105] Only by initiating a rulemaking on AI can the Federal Trade Commission preserve the rights of American consumers, defend American values, protect privacy, and promote civil rights.[106]

CONCLUSION

For the reasons set forth above, the Commission should conduct a trade regulation rulemaking under 15 U.S.C. § 57a concerning the use of artificial intelligence in commerce.

Respectfully Submitted,

MARC ROTENBERG
EPIC President and Executive Director

ALAN BUTLER
EPIC General Counsel

JOHN DAVISSON
EPIC Counsel

CHRISTINE BANNAN
EPIC Consumer Protection Counsel

BEN WINTERS
EPIC Equal Justice Works Fellow

ELECTRONIC PRIVACY
INFORMATION CENTER

[104] *LabMD, Inc. v. FTC*, 894 F.3d 1221, 1227 (11th Cir. 2018).
[105] Rotenberg, *supra* note 7.
[106] Kratsios, *supra* note 38.

1519 New Hampshire Avenue, N.W.
Washington, D.C. 20036
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)