epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

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

Comments of the
ELECTRONIC PRIVACY INFORMATION CENTER

FEDERAL TRADE COMMISSION
Hearings on Competition and Consumer Protection in the 21st Century

Question 9: Consumer Welfare Implications Associated with the Use of Algorithmic Decision Tools, Artificial Intelligence, and Predictive Analytics

August 20, 2018

By notice published on June 20, 2018,[1] the Federal Trade Commission ("FTC") requests public comments on "the consumer welfare implications associated with the use of algorithmic decision tools, artificial intelligence, and predictive analytics." Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits the following comments to address the risks of algorithmic decision tools and urge the FTC to increase accountability for the automated processing of personal data through algorithmic transparency.

Specifically, EPIC urges the FTC to (1) prohibit unfair and deceptive algorithms, (2) seek legislative authority for "algorithmic transparency" to establish consumer protection in automated decision-making, (3) provide guidance on the ethical design and implementation of algorithms, and (4) require the publication of the algorithm – the "Universal Tennis Rating" – that makes possible the secret and unaccountable scoring of young athletes.

EPIC is a public interest research center located in Washington, D.C. EPIC focuses on emerging privacy and civil liberties issues and is a leading consumer advocate before the FTC. 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.[2] EPIC has advocated for

[1] Federal Trade Commission, Press Release, *Federal Trade Commission Announces Hearings on Competition and Consumer Protection in the 21st Century* (June 20, 2018), https://www.ftc.gov/news-events/press-releases/2018/06/ftc-announces-hearings-competition-consumer-protection-21st.

[2] *See, e.g.*, Agreement Containing Consent Order, *In re* Google, Inc., FTC File No. 102-3136 (Mar. 30, 2011); EPIC Complaint, *In re* Google, Inc., FTC File No. 102-3136 (Feb. 16, 2010), http://epic.org/privacy/ftc/googlebuzz/GoogleBuzz_Complaint.pdf; Agreement Containing Consent Order, *In re* Facebook, Inc., FTC File No. 092-3184 (Nov. 29, 2011); EPIC Complaint, *In re* Facebook, Inc., FTC File No. 092-3184 (Dec. 17, 2009), https://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf; EPIC Request for Investigation, *In re* Choicepoint, Inc., FTC File No. 052-3069 (Dec. 16, 2004), http://epic.org/privacy/choicepoint/fcraltr12.16.04.html; EPIC Complaint, *In re* Microsoft Corp., FTC File No. 012-3240 (July 26, 2001), http://epic.org/privacy/consumer/MS_complaint.pdf;

Algorithmic Transparency to ensure fairness in automated decision-making.[3] In 2018, EPIC urged Congress to require algorithmic transparency for dominant Internet firms to ensure media pluralism and fairness in online content.[4] EPIC has also submitted complaints to the FTC to prohibit the use of proprietary algorithms to score young athletes.[5] Internationally, EPIC has advised the UK Information Commissioner's Office and Irish Data Protection Commission on enforcement policies to protect individual rights against algorithmic profiling and discrimination.[6]

I. Increased Reliance on Algorithms and the Impact on Consumers and Society

1. Denial of Fundamental Rights and Opportunities

The proliferation of algorithmic decision tools for governmental and commercial use threatens the exercise of rights that underpin individual autonomy and liberty. Algorithms can collect and analyze unprecedented volumes of personal data to produce predictions, decisions, and content filters that have real life consequences for individuals. However, the "logic" applied to these outcomes are unpredictable, unreliable, and often unexplainable—meaning that individual opportunities and freedoms are being arbitrated by artificial intelligence ("AI") without a clear chain of human liability or accountability.

This is particularly concerning as algorithms often make adverse decisions about people. Algorithms deny people educational opportunities, employment, housing, insurance, and credit.[7] Many of these decisions are entirely opaque, leaving individuals to wonder whether the decisions were accurate, fair, or even about them. Yet there are currently no standards for ethical AI design and implementation in the United States that examine the effect of algorithms on individual

---

EPIC Complaint, *In* re DoubleClick, Inc., FTC File No. 071-0170 (Feb. 10, 2000), http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf; Letter from EPIC Exec. Dir. Marc Rotenberg to FTC Comm'r Christine
Varney (Dec. 14, 1995) (urging the FTC to investigate the misuse of personal information by the direct marketing industry), http://epic.org/privacy/internet/ftc/ftc_letter.html.

[3] EPIC, *Algorithmic Transparency: End Secret Profiling*, https://epic.org/algorithmictransparency/.

[4] EPIC Letter to Chairman Goodlatte and Ranking Member Nadler, *Hearing on Filtering Practices of Social Media Platforms* (April 25, 2018), https://epic.org/testimony/congress/EPIC-HJC-SocialMediaFiltering-Apr2018.pdf.

[5] EPIC Complaint to FTC, *In re Universal Tennis* (May 17, 2017) https://epic.org/algorithmic-transparency/EPIC-FTC-UTR-Complaint.pdf; *See also, In the Matter of Universal Tennis, LLC* (EPIC re-submission of complaint) (May 22, 2018), https://epic.org/algorithmic-transparency/EPIC-FTC-Universal-Tennis-05-2018.pdf.

[6] EPIC, *Comments to the UK Information Commissioner's Office on Data Protection Impact Assessment Draft Guidance* (April 12, 2018), https://epic.org/algorithmic-transparency/EPIC-ICO-Comment-GDPR-DPIA.pdf

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

liberty and the collective interests of society. Therefore, the speed of AI innovation and its impact on society necessitate urgent ethical and regulatory review by the FTC.

2. Unfair and Deceptive Practices in Secret Algorithms

Accountability is key to a fair decision-making process. But as decisions are automated, and organizations increasingly delegate decision-making to techniques they do not fully understand, processes become more opaque and less accountable. Consumers have a right to know the data processes that impact their lives so they can correct errors and contest decisions made by algorithms. These opaque, automated decision-making processes bear risks of secret profiling and discrimination as well as undermine our privacy and freedom of association. It is timely for the Commission to address this now, as reliance on secret algorithms is rapidly increasing in the United States and worldwide:

Evidence strongly suggests that consumer scoring mechanisms have widespread discriminatory impacts.[8] Algorithms reflect and reinforce the historical discrimination that is present in the data sets they rely on, as well as the human biases of the individuals who develop them.[9]

a. Illicit Microtargeting

- Algorithms have also allowed advertisers to engage in racial targeting. Facebook's algorithms, for example, allowed marketers for the film "Straight Outta Compton" to show different advertisements to users based on their "racial affinity."[10]

- Algorithms can target political ads to individuals with unprecedented granularity; this technique poses serious threats on the democratic process. The technology surpasses the reach of traditional media and necessitates greater disclosure requirements from online advertisers, as algorithms can be misused for disinformation campaigns that propagate divisive messages to demographic targets and disrupt democratic elections. The investigations of the UK Information Commissioner's Office ("ICO") on Facebook and Cambridge Analytica found that the "invisible processing" of personal data for political microtargeting on social media enabled foreign interference and illicit social engineering

[8] *See*, FRANK PASQUALE, THE BLACK BOX SOCIETY 8 (2015); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 Wash. L. Rev. 1 (2014).
[9] Cathy O'Neil, *Weapons of Math Destruction* (2016)
[10] Alex Hern, *Facebook's 'ethnic affinity' advertising sparks concerns of racial profiling*, The Guardian (March 22, 2016), https://www.theguardian.com/technology/2016/mar/22/facebooksethnic-affinity-advertising-concerns-racial-profiling.

during the EU Referendum on Brexit and the 2016 U.S. Presidential Campaign.[11] A key finding of the ICO investigation was that "Facebook has not been sufficiently transparent to enable users to understand how and why they might be targeted by a political party or campaign."[12]

- Algorithmic transparency on the use of data analytics by political entities is critical to the integrity of democratic institutions. Regulatory agencies should obligate full disclosures on how an advertiser used its tools to create a target audience for that advertisement, including what data it collected about the user that caused the user to be placed within that target audience. These disclosures would establish accountability for the use of online political advertising and help users evaluate the arguments to which they are being subjected.

b. Network Discrimination

- Algorithms enable credit companies to discriminate against loan applicants based on their personal network. For example, a credit company called Kreditech deploys a proprietary credit-scoring algorithm to process up to 20,000 data points on the loan applicant's social media networks, ecommerce behavior, and web analytics.[13] Information about the applicant's social media friends are collected to assess the applicant's "decision-making quality" and creditworthiness. Kreditech's Chief Financial Officer, Rene Griemens, told the Financial Times that being connected to someone who has already satisfied a loan with the company is "usually a good indicator."[14] Algorithms that make adverse inferences on individuals by assessing their interpersonal network pose new threats of inequitable treatment and discrimination based on freedom of association.

- Fair Isaac Corp ("FICO") is partnering with startups like Lenddo to process large quantities of data from the applicant's mobile phone to conduct predictive credit-risk assessments.[15] Lenddo collects longitudinal location data to verify the applicant's

[11] UK Information Commissioner's Office, *Investigation into the use of data analytics in political campaigns* (July 11, 2018), https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf

[12] UK Information Commissioner's Office, *Democracy Disrupted? Personal Information and Political Influence* (July 11, 2018), https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf.

[13] See, Kreditech, What We Do, https://www.kreditech.com/what-we-do/.

[14] Jeevan Vasagar, *Kreditech: A Credit Check by Social Media: Hamburg-Based Start-Up Uses Algorithms to Help It Assess Borrowers' Trustworthiness,* Financial Times (Jan. 19, 2016), https://www.ft.com/content/12dc4cda-ae59-11e5-b955-1a1d298b6250

[15] Kaveh Waddell, *How Algorithms Can Bring Down Minorities' Credit Scores,* The Atlantic, Dec. 2, 2016, https://www.theatlantic.com/technology/archive/2016/12/how-algorithms-can-bring-down-minorities-credit-scores/509333/; *See also*, Olga Kharif, *No Credit History? No Problem. Lenders Are Looking at Your Phone Data*, Bloomberg Markets (Nov. 25, 2016),

residence and work address, then analyzes the applicant's interpersonal communications and associations on social media to produce a credit score.[16] Secret profiling based on personal web activity infringes the fundamental rights to privacy and access to information, but it is perilously becoming normalized and rebranded as "online verification methods."

c. Lack of Due Process

- Algorithms in the consumer lending context may also violate the law.[17] The Equal Credit Opportunity Act ("ECOA") prohibits lenders from basing credit decisions on factors that have a discriminatory impact on protected groups and are unrelated to creditworthiness.[18] If credit reporting agencies are permitted to score consumers using secret, proprietary algorithms, then it is impossible to know whether these algorithms violate the law.

- Credit scores by their very nature "bake in and perpetuate past discrimination"; they judge consumers based on their histories and consequently limit or expand their future ability to obtain wealth-building assets such as a home, a small business loan, or even a job.[19] Yet current law does not allow regulators or the courts to scrutinize these scores to determine whether they violate ECOA.[20] Although consumers have the right to request their credit scores, they do not have the right to know how this score is determined.[21]

d. Price Discrimination

- Algorithms can facilitate price discrimination. Amazon has deployed algorithms to assess the socio-economic and racial demographics of neighborhoods and excluded same-day delivery services to predominantly poor and African American neighborhoods in Boston,

---

https://www.bloomberg.com/news/articles/2016-11-25/no-credit-history-no-problem-lenders-now-peering-at-phone-data.

[16] Porter Novelli, *FICO and Lenddo Partner to Extend Credit Reach in India,* FICO (Oct. 3, 2016), http://www.fico.com/en/newsroom/fico-and-lenddo-partner-to-extend-credit-reach-in-india-10-03-2016; *See also*, Lenddo, *Our Products, Credit Scoring: The LenddoScore,* https://www.lenddo.com/products.html#creditscore.

[17] Citron & Pasquale, *supra*, note 47.

[18] 15 U.S.C. § 1601 et seq.

[19] *Past Imperfect: How Credit Scores and Other Analytics "Bake In" and Perpetuate Past Discrimination*, National Consumer Law Center, (May 2016), https://www.nclc.org/images/pdf/credit_discrimination/Past_Imperfect050616.pdf.

[20] *Id.*

[21] Citron & Pasquale, *supra*, note 47

Atlanta, Chicago, Dallas, New York City and Washington, which it determined were "not profitable areas for the business."[22]

e. Citizen Scoring

- Algorithms are used for social control. The Chinese government is deploying a "social credit" system that assigns to each person a government-determined favorability rating. "Infractions such as fare cheating, jaywalking, and violating family-planning rules" would affect a person's rating.[23] Low ratings are also assigned to those who frequent disfavored web sites or socialize with others who have low ratings. Citizens with low ratings will have trouble getting loans or government services. Citizens with high ratings, assigned by the government, receive preferential treatment across a wide range of programs and activities.

Without knowledge of the factors that provide the basis for decisions, it is impossible to know whether government and companies engage in practices that are deceptive, discriminatory, or unethical. Additionally, if there is no right to be informed of the application automated decision-making to one's personal data and the likely consequences of processing, then consumers cannot avoid the potential harms of the algorithm. Therefore, algorithmic transparency is crucial to defending human rights and democracy online.

The FTC should fully apply its existing authority to protect consumers from the detrimental effects of algorithmic decision tools and seek legislative support from Congress to modernize its jurisdiction on emerging AI technology. We make the following recommendations:

II. Policy Recommendations: FTC Regulatory Strategy on Algorithms and AI

1. Use Section 5 Authority for Algorithmic Transparency and Accountability

Unfair and deceptive algorithms are prevalent because the current lack of regulatory oversight has allowed companies to prioritize the commercial advantages of AI while externalizing its risks to individual rights, freedoms, and the collective society. Secret algorithms are proliferating because institutions evade rigorous testing of their computational models by hiding behind technical excuses (arguing that algorithmic transparency is impossible due to the complexity and fluidity of modern processes), economic justifications (the cost of preparing an explanation that can be rationalized by a human is prohibitive), and legal interests (opacity is

[22] David Ingold and Spencer Soper, Amazon Doesn't Consider the Race of Its Customers. Should It?, Bloomberg (April 21, 2016), https://www.bloomberg.com/graphics/2016-amazon-same-day/.
[23] Josh Chin & Gillian Wong, China's New Tool for Social Control: A Credit Rating for Everything, Wall Street J. (Nov. 28, 2016), http://www.wsj.com/articles/chinas-new-tool-forsocial-control-a-credit-rating-for-everything-1480351590

necessary to protect intellectual property rights and trade secrets). However, algorithmic opacity should never be accepted as the norm, and automated decision-making systems should evolve through public scrutiny.

International legal frameworks recognize that the touchstone of algorithmic transparency is the responsibility of institutions to justify the provability of their own analytic systems and to address potential and actualized harms. The EU General Data Protection Regulation ("GDPR") establishes legal and regulatory measures to contest automated decisions, and enforcement mechanisms to end opaque practices that threaten fundamental rights.[24] The GDPR empowers the national Data Protection Authorities ("DPAs") to protect individual rights against algorithmic profiling and discrimination caused by automated processing.

Equally, there must be a U.S. regulatory framework to ensure fairness in automated processing and the right to explanation of the logic of processing. Actionable measures are necessary for individuals to examine the algorithm's "logic process" and the factors contributing to an automated decision, to provide an opportunity to rectify inaccurate information or machine-learning biases. Algorithmic transparency is critical to the protection of individual rights, because even accurate input can be distorted by a particular analytic model to extrapolate biased inferences that result in profiling and algorithmic discrimination. Therefore, algorithms must always be open for review and public scrutiny.

a. Prohibit Algorithmic Decision Tools that Risk Individual Rights and Freedoms

Using its broad mandate to police unfair and deceptive practices, the FTC must be at the forefront of establishing accountability in algorithms and AI. Automated systems rely on probabilistic and emergent designs that can significantly harm consumers without the appropriate regulatory oversight. The FTC must oversee the fairness and accuracy of the input of algorithms, and require transparency for the rationale of automated decisions. Without these relevant safeguards, the deployment of algorithms can easily lead to unfair and deceptive practices which silently and pervasively threaten individual rights and equitable access to opportunities. Secret algorithms that pose risks on consumers' rights and opportunities are unfair and deceptive, and must be promptly investigated and prohibited by the FTC.

The FTC must start by bringing more enforcement actions against unfair and deceptive uses of algorithmic decision tools. The Commission should adopt a broad understanding of

[24] EPIC Comments to UK Information Commissioner's Office, *Consultation on Data Protection Impact Assessments (DPIAs) Guidance* (Apr. 12, 2018), https://epic.org/algorithmic-transparency/EPIC-ICO-Comment-GDPR-DPIA.pdf

"consumer harm" caused by companies that fail to be transparent and accountable for their algorithms that produce decisions on individuals. In particular:

- The FTC should not impose an unreasonable evidentiary burden on "injury" to bring a complaint against a secret algorithmic decision tool.

- The FTC should establish and enforce formal procedures for the access to and rectification of inaccurate, incomplete, and outdated data input for algorithms.

    - Consumers should have the right to contest an automated decision is actionable even if the algorithm was applied to a group rather than an individual.

- The FTC should require companies to make public the algorithm and other machine learning techniques that produce automated decisions.

    - Consumers should have the right to an explanation of the "logic of the algorithm" even if the algorithm merely factored into the automated decision-making without actually making the decision. Moreover, the fact that a decision was not "solely" based on the algorithm should not preclude a claim.

The FTC should also timely respond to complaints on algorithmic decision tools filed by consumer groups and civil society. EPIC has repeatedly urged the Commission to act on a complaint previously filed with the FTC about the secret scoring of young tennis players.[25] The EPIC complaint concerns Universal Tennis Rating ("UTR"), a proprietary algorithm used to assign numeric scores to tennis players, many of whom are children under 13. EPIC emphasized that "the UTR score defines the status of young athletes in all tennis-related activity; impacts opportunities for scholarship, education and employment; and may in the future provide the basis for 'social scoring' and government rating of citizens."[26]

The Commission should prohibit this algorithmic decision tool as an unfair trade practice. Injury cannot be reasonably avoided because parents are not allowed to opt out of UTR scoring, and the harms from the use of this secret algorithm are not outweighed by countervailing benefits to consumers or to competition. It is the FTC's responsibility to investigate the complaints filed by consumer groups to apply its Section 5 authority[27] and prohibit companies from deploying

[25] EPIC, *EPIC Asks FTC to Stop System for Secret Scoring of Young Athletes* (May 17, 2017), https://epic.org/2017/05/epic-asks-ftc-to-stop-system-f.html; *See also* Shanya Possess, *Privacy Group Challenges Secret Tennis Scoring System*, Law360, May 17, 2017, https://www.law360.com/articles/925379; Lexology, *EPIC Takes a Swing at Youth Tennis Ratings*, June 1, 2017, https://www.lexology.com/library/detail.aspx?g=604e3321-dfc8-4f46-9afc-abd47c5a5179

[26] EPIC Complaint to Federal Trade Commission, In re Universal Tennis at 1 (May 17, 2017).

[27] Federal Trade Commission Act, 15 U.S.C. § 46 (2006).

secret algorithms without data protection requirements—such as data minimization, data accuracy, auditability, explanation of processing, and right to redress.

The Commission has the legal authority to prohibit such algorithms and build stronger standards for ethical AI design and implementation under Section 5.[28] It should use its authority to prosecute unfair and deceptive practices to accomplish algorithmic transparency and accountability.

2. Seek Legislative Authority for Consumer Protection in Algorithms

Additionally, the FTC should seek legislative authority to protect consumers against algorithmic profiling and discrimination. Congressional action is overdue on expanding the powers of regulatory agencies to address the new challenges posed by AI. The FTC needs to testify before Congress in support of privacy legislation that would allow the Commission to supervise the development and deployment of algorithms with pre-market audits, design standards, and risk evaluations.

The FTC needs additional powers to safeguard consumers against algorithmic profiling and discrimination by the right to examine the design, implementation, and consequences of automated processing. Congress should establish a broad mandate for the Commission to enforce algorithmic transparency and accountability for the use of data that produces automated decisions. This mandate should emphasize accessibility and accountability:

a. Accessibility

- Individuals should have the right to be informed of being subject to algorithmic decision tools, and the right of access to the input data and an explanation of how they factored into the decision.

- The Commission should have full authority to establish checkpoints for transparency and accuracy at each automated processing stage to improve data governance, data quality, and the opportunity to correct hidden bias. Further data protection authority is imperative to oversee the quantity, quality, and relevance of the data chosen as input for algorithms. Oversight of the data input for algorithmic decision tools is fundamental to identifying bias and inaccuracy to avert unfair outcomes.

b. Accountability

- Consumers should have a right to invoke remedies and obtain redress from adverse decisions made by algorithms. Algorithmic transparency requires institutions to justify

[28] *Id. See also*, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3rd Cir. 2015).

the provability of their own analytic systems and to address potential and actualized harms. The FTC should enable consumers to contest automated decisions, and bring enforcement action to end unfair secret algorithms that threaten fundamental rights.

We suggest the following checkpoints for a legal and regulatory framework that ensures algorithmic transparency and accountability:

- Laws or regulations for data controllers to notify individuals when their personal data is being processed for automated decision-making.
- Further notification requirements on the purpose and extent of the processing, and an explanation of the envisaged consequences of the automated decision.
- Decision-making algorithms should identify itself to the subject and explain the personal data collected for processing and how they will be weighed to make determinations.
- Comprehensive legal standards on data provenance, quality, and relevance.
- Individuals should have the ability to examine the lawfulness or validity of processing, and have recourse to invoke legal remedies.
- Public record of validation and testing of computational models used for input and output.
- Clear legal and regulatory standards on the extent of disclosure required for the "logic of the process" and what qualifies as a "meaningful explanation" of decisions.
- Regulation to limit secondary uses of data collected for automated processing, and enforcement action against companies that do not maintain records of the specific purposes of data processing or exceed their stated purpose.
- The right to contest an automated decision is actionable even if the algorithm was applied to a group rather than an individual.
- The rights to explanation and redress should be actionable even if the algorithm merely "factored into" the automated decision-making without actually making the decision.
- Engagement of third party auditors where harm is suspected from automated processes.
- Implementation of machine learning to differentiate correlation and causation to improve the accuracy of automated decisions.

- Prohibition of algorithms that are essentially unprovable and logically inconsistent. Requirement of testing on intercoder reliability to establish replicability of outcomes.

- Legal protection against automated decision-making by default, where the data processor must prove an exemption to the prohibition through contract or explicit consent.

- If transparency is achievable with an alternative system based on objective and provable metrics, then proprietary algorithms should not be deployed.

3. Research and Establish Guidelines on Ethical Algorithms

The FTC should research and produce guidelines on the ethical design and implementation of algorithms. The Commission should establish best practice guidelines to improve the design of algorithmic systems to further consumer protection and eliminate the risks to privacy, free expression, and democratic institutions.

Significant ethical issues emerge from the increased deployment of algorithmic decision tools due to the incorrect perception that AI is more efficient and predictable than human judgement. Algorithms and machine learning, and the secrecy surrounding their inner workings, have eroded a sense of human responsibility for decisions that impact human lives. The FTC must work with civil society groups and consumer advocates to increase public vigilance on the impact of AI. In particular, the FTC should examine the following risks:

a. Unclear Liability for Machine-Delegated Decisions

- Delegating decision-making authority to AI poses a threat to human autonomy and free will. Algorithmic decision tools employ deterministic or self-learning techniques that lack human judgment, empathy, and the ability to manage exceptions to a set of rules. Self-learning neural networks easily become blackboxes where the decision-making process becomes incomprehensible to the designers themselves. This poses serious concerns for the chain of liability for unfair and discriminatory decisions produced by AI, and whether the liability belongs to the developer, designer, training data provider, or the end user of the product.

b. Profiling, Bias, and Discrimination

- Algorithms can replicate bias and historical discrimination. The French Data Protection Authority ("CNIL") warns that AI is never neutral because it reflects societal categories that we choose to input, and this input can incorporate bias and stereotypes.[29]

[29] Commission Nationale de l'Informatique et des Libertés (CNIL), *HOW CAN HUMANS*

- Algorithms have a multiplier effect on bias due to the scale and frequency of deployment for decision-making. The FTC should ensure that algorithms are not configured with biased, inaccurate, and discriminatory training data or operating criteria to produce these detrimental effects on individuals and democratic society at large. AI must be checked for sensitive data processing so that it does not become a vehicle for racial and socio-economic profiling. It is critical that AI incorporate democratic values and respect for fundamental rights.

c. Restrictive Standardization

- Algorithms are often deployed to filter potential candidates for employment and admission to academic institutions. Without human intervention, AI is unable to contemplate exceptions for candidates that may not meet the pre-determined criteria but still show excellent qualities for the position in other regards.

- There is a risk for normativity and restriction through the standardization of criteria used in these algorithmic decision tools. The FTC should examine the effect of "filter bubbles" on employment and admissions, and set guidelines to ensure that pre-determined profiles and superficial checkpoints do not close off opportunities for under-represented and under-privileged groups.

d. Segmentation as a Threat to Democratic and Cultural Pluralism

- Filtering algorithms can prevent individuals from using the Internet to exchange information on topics that may be controversial or unpopular.

- The majority of users are unaware of how algorithmic filtering restricts their access to information and do not have an option to disable filters. This can diminish the quality of public debate, fragment political messaging, and significantly curtail the diversity of information presented to users. The FTC should examine how companies are externalizing large-scale political and cultural effects of their algorithms, and the impact on access to information and democratic pluralism.

e. Data Protection for Algorithmic Input

- Algorithms process immense quantities of personal data to "improve" machine learning, but rarely follow Fair Information Practices. Algorithms must observe data protection principles in the collection and processing of personal data to ensure selection rigor for the quantity, quality, and relevance of input data. Stronger data protection for AI would

---

KEEP THE UPPER HAND? The ethical matters raised by algorithms and artificial intelligence (December 2017), https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf

reduce the methodological negligence of processing systems that produce inaccurate and unreliable results.

- The FTC should promulgate standards for data minimization and limit data retention periods for algorithms.

Conclusion

The FTC is empowered to impose standards for algorithmic transparency and accountability under Section 5.[30] Secret algorithms are inherently unfair and deceptive, as they make automated decisions that impact individuals without accountability and transparency. They conceal discriminatory and anti-competitive practices, and deprive consumers of opportunities to make meaningful decisions in the marketplace.

The Commission has a critical role in ensuring that AI development prioritizes fairness and openness. To ensure algorithmic accountability, the FTC must ensure the transparency of decisions concerning individuals. Therefore, algorithmic transparency should be central to the FTC's future regulatory strategy.

Respectfully Submitted,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Sunny Seon Kang*
Sunny Seon Kang
EPIC International Consumer Counsel

[30] *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3rd Cir. 2015).