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

Federal Trade Commission

Draft FTC Strategic Plan for FY 2022-2026

Docket No. FTC-2021-0061

November 30, 2021

The Electronic Privacy Information Center (EPIC) submits these comments in response to the Federal Trade Commission (FTC)'s Draft Strategic Plan for Fiscal Year 2022-2026.[1] EPIC applauds the Commission's efforts to advance racial equity and its acknowledgment that safeguarding consumer privacy is a key component of the FTC's mission. However, EPIC urges the Commission to (1) elevate the protection of privacy to a separate objective in the Strategic Plan, and (2) set metrics for the Commission's efforts to enhance privacy with a focus on racial equity.

I. The FTC should elevate privacy protection to a separate objective in the Strategic Plan, drawing on the recent work of EPIC and peer organizations as a blueprint.

Although the Strategic Plan correctly notes the FTC's obligation to safeguard consumer privacy, the Plan offers almost no information about the Commission's strategy for pursuing this goal. Given the deepening crisis of exploitative data practices this country faces, the Commission should break out data protection as a separate objective and use this opportunity to outline its long-term approach to consumer privacy.

[1] Fed. Trade Comm'n, Draft FTC Strategic Plan for FY 2022-2026 (Nov. 11, 2021), https://www.regulations.gov/docket/FTC-2021-0061.

Over the last few years, EPIC and coalition partners have provided the FTC with resources the Commission can rely on to protect privacy and safeguard consumers online. EPIC published a letter outlining what the Commission should prioritize in the presidential transition.[2] In February 2020, EPIC submitted a rulemaking petition calling for the FTC to regulate commercial artificial intelligence products by enforcing the guidelines laid out in the OECD AI Principles,[3] and the Universal Guidelines for AI.[4] EPIC's petition detailed the widespread use of AI decision-making in commercial settings and the harms that result from biased and inaccurate algorithms. EPIC subsequently launched its Screening and Scoring Project, which seeks to document misuse of algorithmic decision-making tools and protect the public from harmful AI.[5]

In November 2020, EPIC and coalition partners published a letter outlining what the new administration should prioritize in the presidential transition, including recommendations for the FTC's protection of privacy.[6]

In March 2021, EPIC and a coalition of nearly 40 other groups launched a campaign to Ban Surveillance Advertising.[7] The campaign centers the cross-cutting harms created by Big Tech's surveillance advertising model, including mainstreaming misinformation that damages public health, selling access to sensitive information to third parties and governments, stifling innovation, disadvantaging small businesses, and promoting scams to wide and often vulnerable audiences.[8]

---

[2] EPIC, In Re: Petition for Rulemaking Concerning Use of Artificial Intelligence in Commerce (Feb. 2020), https://epic.org/wp-content/uploads/privacy/ftc/ai/EPIC-FTC-AI-Petition.pdf.
[3] OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449 (May 22, 2019), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.
[4] The Public Voice, *Universal Guidelines for Artificial Intelligence* (Oct. 23, 2018), https://thepublicvoice.org/ai-universal-guidelines/.
[5] EPIC, *Screening and Scoring*, https://epic.org/issues/ai/screening-scoring/.
[6] *Privacy and Digital Rights for All* (Nov. 10, 2020), https://epic.org/wp-content/uploads/privacy/policy/Privacy-And-Digital-Rights-For-All-A-blueprint-for-the-next-Administration.pdf.
[7] Ban Surveillance Advertising, https://www.bansurveillanceadvertising.com.
[8] *The Real Costs of the Business*, Ban Surveillance Advertising, https://www.bansurveillanceadvertising.com/real-costs-of-the-business.

In June, EPIC published a report on the Commission's unused and underused statutory authorities, urging the Commission to make full use of its powers to safeguard privacy.[9] EPIC's report provides a toolkit for the FTC to establish a regulatory framework for data protection and to undertake meaningful privacy enforcement actions that will protect consumers and deter bad actors.

In August, EPIC and a coalition of 23 public interest, consumer advocacy, and civil rights groups sent a letter to the FTC laying out the broad range of exploitative commercial data practices demanding the Commission's attention and the harms that those practices cause.[10]

In October, EPIC and a coalition of 44 consumer advocacy, civil rights, and media democracy groups urged the FTC to initiate a rulemaking to promote civil rights and protect against abusive data practices.[11]

In sum, EPIC and peer organizations have already mapped out the ways in which the FTC must take the lead in regulating privacy, data protection, and artificial intelligence. The Commission can start to implement these recommendations by prioritizing privacy in the agency's Strategic Plan for 2022-2026.

II. The FTC should set definite consumer privacy metrics and center the privacy harms suffered by marginalized communities in its Strategic Plan.

With each passing year, more and more individuals are harmed by data exploitation, opaque and discriminatory algorithmic decision-making, and shoddy data protection practices. Although EPIC continues to believe that the United States needs a national data protection agency (DPA), Congress has so far failed to act.[12] In the absence of a DPA, the FTC is the main federal agency

[9] EPIC, *What the FTC Could Be Doing (But Isn't) To Protect Privacy: The FTC's Unused Authorities* (June 2021), https://epic.org/wp-content/uploads/privacy/consumer/EPIC-FTC-Unused-Authorities-Report-June2021.pdf.
[10] Letter from Public Interest Groups to Lina Khan, Chair, Fed. Trade Comm'n, et al. (Aug. 4, 2021), https://www.publicknowledge.org/documents/public-interest-group-ftc-privacy-letter/.
[11] Letter from Public Interest Groups to Lina Khan, Chair, Fed. Trade Comm'n, et al. (Oct. 27, 2021), https://www.freepress.net/sites/default/files/2021-10/Letter-to-FTC-on-Privacy-Rulemaking-10-27-2021.pdf.
[12] EPIC, *The U.S. Urgently Needs a Data Protection Agency* (2020), https://epic.org/dpa/.

responsible for online privacy enforcement. The Commission should fully embrace this role in the Strategic Plan, setting clear metrics for its privacy protection efforts and laying out its approach to preventing and remedying the harms of abusive data practices that disproportionately affect vulnerable populations.

a. The Commission should establish clear benchmarks for its privacy protection work.

The Commission recognizes that privacy is an important element of the agency's work and mission. The Draft Strategic Plan identifies investigating and litigating privacy injuries as a core component of its first strategic goal (protecting the public from unfair and deceptive practices).[13] The Plan therefore incorporates "safeguarding consumer privacy" as an element of Objective 1.1 (investigating and deterring unfair and deceptive trade practices) and Objective 1.3 (collaborating to enhance consumer protection).[14]

Despite the Commission's recognition of the central role privacy plays in its enforcement mission, the document fails to set any specific metrics for determining whether the Commission has met its privacy objectives. These metrics could include, for example, the number of enforcement actions initiated against companies for unfair, deceptive, or otherwise unlawful data practices, the amount collected in civil penalties from such companies, the number of businesses placed on notice of their data protection obligations, the number of consumers who obtain redress through the FTC, and the number of abusive data practices declared unfair or deceptive through policy statements and/or trade regulation rulemakings. Yet the strategic plan includes no such benchmarks.

Without definite metrics for privacy enforcement, it is unclear how aggressively the Commission intends to act to safeguard consumer privacy. And neither the public nor the Commission itself can hold the FTC accountable for failing to meet metrics that do not exist. The

[13] Draft Strategic Plan at 5.
[14] *Id*. at 9, 13.

FTC's enforcement work is also likely to suffer unless the Commission sets goals for, and keeps track of, each facet of its privacy protection efforts.

b. Protecting privacy is necessary to advance racial equity and support minority communities.

The Strategic Plan states that the FTC will prioritize advancing racial equity and supporting underserved and minority communities.[15] Following that objective, the FTC will target practices that "disproportionately affect historically underserved and marginalized communities."[16] EPIC supports the Commission in its renewed focus on underserved communities. However, to fully meet its goal of stopping and remedying harms to marginalized communities, the Commission also needs to address privacy.

Although data exploitation, junk-science algorithmic decision-making, corporate surveillance, and lax data protection can harm everyone, low-income and marginalized communities are usually the hardest hit. Members of these communities are subject to the most coercive economic pressures, have the least time available to research personal privacy practices, and often cannot pay a premium for more privacy-protective services. When data breaches occur, people living on the margins are the most impacted.[17]

Marginalized communities are also disproportionately targeted for the worst effects of data exploitation, algorithmic bias, and predatory pricing for digital services. The effects of unregulated and nonconsensual location data mining fall heaviest on Black, immigrant, and Muslim communities. Black communities in the U.S. are disproportionately policed and disproportionately subjected to surveillance. Police use of advanced surveillance technologies like facial recognition—

[15] *Id*. at 14.
[16] *Id*.
[17] Mary Madden, *The Devastating Consequences of Being Poor in the Digital Age*, N.Y. Times (Apr. 25, 2019), https://www.nytimes.com/2019/04/25/opinion/privacy-poverty.html.

technologies that are often built on non-consensual data mining,[18]—create the greatest risk for marginalized communities.[19] And law enforcement agencies are fast becoming major buyers of bulk location data.[20] For example, federal immigration enforcement agencies are also major clients of location data broker Venntel Inc.[21] Location data mining is always harmful, but sale of this data poses a much greater threat to undocumented immigrants subjected to U.S. Immigration and Customs Enforcement raids than almost any other community. Apps harvesting location data without meaningful consent, and often even when users think they've disabled location tracking,[22] are often aimed at Muslims. Muslim prayer apps including Salaat First,[23] Qibla Compass,[24] Muslim Pro, and dating app Muslim Mingle[25] all sent location data to large data brokers contracting with the U.S. military and government agencies.

[18] For example, Clearview AI has amassed a database of more than 10 billion facial recognition images tied to social media profiles. Those images were scraped from social media sites, violating their terms of service and in some countries violating privacy laws. Clearview's main customers are law enforcement agencies. *See*, Ryan Mac, Caroline Haskins, & Logan McDonald, *Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA*, Buzzfeed News (Feb. 27, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement; James Vincent, *Clearview AI ordered to delete all facial recognition data belonging to Australians*, The Verge (Nov. 3, 2021), https://www.theverge.com/2021/11/3/22761001/clearview-ai-facial-recognition-australia-breach-data-delete; Ryan Mac, Clearview AI, a facial recognition company, is fined for breach of Britain's privacy laws., N.Y. Times (Nov. 29, 2021), https://www.nytimes.com/2021/11/29/technology/clearview-ai-uk-privacy-fine.html.

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

[20] https://www.vox.com/recode/22038383/dhs-cbp-investigation-cellphone-data-brokers-venntel; https://www.wired.com/story/opinion-data-brokers-know-where-you-are-and-want-to-sell-that-intel/.

[21] Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, Wall St. J. (Feb. 7, 2020), https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600.

[22] Joseph Cox, *Location Data Firm Got GPS Data From Apps Even When People Opted Out*, Vice (Oct. 25, 2021), https://www.vice.com/en/article/5dgmqz/huq-location-data-opt-out-no-consent.

[23] Joseph Cox, *Leaked Location Data Shows Another Muslim Prayer App Tracking Users*, Vice (Jan. 11, 2021), https://www.vice.com/en/article/xgz4n3/muslim-app-location-data-salaat-first.

[24] Joseph Cox, *Location Data Firm Got GPS Data From Apps Even When People Opted Out*, Vice (Oct. 25, 2021), https://www.vice.com/en/article/5dgmqz/huq-location-data-opt-out-no-consent.

[25] Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, Vice (Nov. 16, 2020), https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x.

Investigations of the Facebook Papers recently revealed that Facebook knowingly employed biased content moderation algorithms, exposing people of color to hate speech while removing "anti-white" content at a much higher rate.[26] Up to 90 percent of the content flagged for removal by was "anti-white" or directed at men even though a substantial majority of hate speech on the site is directed at people of color, the LGBTQ community, Jews, and Muslims.[27] Facebook's newsfeed algorithms also targeted people with low technology literacy with disturbing content, including violence and nudity.[28] In one example of Facebook's harmful content targeting, a person who joined a Narcotics Anonymous group began seeing ads, page recommendations, and posts about alcohol.[29] People with low tech literacy were disproportionately older, poor, or racial minorities. Harmful ad targeting results from overly invasive and unregulated data collection.

The FTC has a critical role to play in ending surveillance advertising and remedying historically disparate impacts of online services. The Strategic Plan must reflect that.

Conclusion

EPIC applauds the FTC's draft Strategic Plan for foregrounding harms to marginalized communities and setting explicit goals to advance racial equity. Yet as the nation's primary consumer privacy enforcement agency, the Commission should also emphasize reining in exploitative commercial data practices to protect individuals from multiplying online threats. Prioritizing privacy would serve the Commission's overarching goal of protecting the public from

[26] Elizabeth Dwoskin, Nitasha Tiku, & Craig Timberg, *Facebook's race-blind practices around hate speech came at the expense of Black users, new documents show*, Washington Post (Nov. 21, 2021), https://www.washingtonpost.com/technology/2021/11/21/facebook-algorithm-biased-race/.
[27] *Id.*
[28] Kenny Jacoby, *Facebook fed posts with violence and nudity to people with low digital literacy*, USA Today (Nov. 23, 2021), https://www.usatoday.com/story/tech/2021/11/23/facebook-posts-violence-nudity-algorithm/6240462001/?gnt-cfr=1.
[29] *Id.*

unfair and deceptive practices, fill a gap in the federal regulatory scheme, and promote equity for underserved and minority communities.

Respectfully Submitted,

Jake Wiener
Jake Wiener
EPIC Law Fellow

John Davisson
John Davisson
EPIC Senior Counsel