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

In the Matter of	)	
	)	
Commercial Surveillance ANPR	)	Docket No. FTC-2022-0053
R111004	)	

COMMENTS OF COMMON CAUSE

Submitted via regulations.gov

I. Introduction and Summary

Common Cause submits these comments in response to the Federal Trade Commission's ("FTC" or "the Commission") Advance Notice of Proposed Rulemaking ("ANPR") requesting public comment on the prevalence of commercial surveillance and data security practices that harm consumers.[1] Common Cause is a nonpartisan, grassroots organization dedicated to upholding the core values of American democracy. We work to create an open, honest, accountable government that serves the public interest; promote equal rights, opportunity, and representation for all; and empower all people to make their voices heard in the political process.

Protection from commercial surveillance is critical to our members. The mass collection of people's data and the use of that data to track and influence their choices creates a myriad of harms to democracy, civil rights, and equal opportunity.

This comment responds to questions 1-12, 30, 43, and 65-72; and may be applicable to others.

Our comments begin with an overview of why the FTC has the authority to conduct this rulemaking, why Section 5 empowers the Commission to regulate the harms and practices discussed below, and why the gaps in industry self-regulation, sector-specific regulation, and state law have created the need for this rulemaking. Next, we discuss a few harms of the surveillance economy - primarily broad harms to our democracy that stem from pervasive fraud online and discriminatory ad targeting, and the civil rights harms that result from algorithmic

[1] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273 (proposed Aug. 22, 2022).

discrimination. Finally, we provide recommendations for a comprehensive set of rules to address the harms described herein, including a data minimization framework, nondiscrimination rules and civil rights protections, individual rights, and transparency requirements.

II. The FTC Act Authorizes and Empowers The FTC to Conduct a Commercial Surveillance and Data Security Rulemaking

Question 30 of the ANPR explicitly asks if the Commission should "pursue a Section 18 rulemaking on commercial surveillance and data security," and inquires about the sufficiency of current legal authority and self-regulation.[2] Last year, Accountable Tech petitioned the Commission for a rulemaking to prohibit surveillance advertising,[3] and several commenters suggested that the Commission address some of the problems mentioned in the petition through a broader data privacy rulemaking.[4] It is clear that existing statutory authority gives the Commission the power to initiate the rulemaking under Section 18 of the FTC Act and regulate commercial surveillance and data security under Section 5 of the FTC act. The approach the Commission seeks to take in this rulemaking is the right one, and would serve to address the gaps left by industry self-regulation, the current sectoral approach to oversee privacy, and the patchwork of existing state laws.

A. Section 5 of the FTC Act Empowers the Commission to Regulate Unfair Deceptive Acts or Practices

Section 5 of the FTC Act allows the Commission to regulate "unfair or deceptive acts or practices." A deceptive act is one that involves a material representation, omission, or practice that is likely to mislead a consumer acting reasonably under the circumstances; an act or practice is considered to be unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers and not outweighed by countervailing benefits to consumers or competition."[5]

Historically, the Commission has used both the deceptive and unfair rationales as a basis to file complaints against companies for privacy violations.[6] With respect to deceptive practices, the FTC has focused on instances where a company violates specific promises within their own

---

[2] *Id.*
[3] Petition for Rulemaking: Accountable Tech, 86 Fed. Reg. 73206 (received Dec. 27, 2021).
[4] *Comments of Public Knowledg*e, Petition for Rulemaking: Accountable Tech, 86 Fed. Reg. 73206 (2022); *Comments of Consumer Reports and the Electronic Privacy Information Center*, Petition for Rulemaking: Accountable Tech, 86 Fed. Reg. 73206 (2022).
[5] 15 U.S.C. Sec. 45(n).
[6] Daniel J. Solove and Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Columbia L. Rev. 584, 627-628 (2014), https://cyberlaw.stanford.edu/sites/default/files/SSRN-id2312913.pdf.

privacy policies or when a company uses false pretenses to induce disclosure of confidential information.[7] Similarly, the FTC has found that deceitful data collection is an unfair practice.[8]

Even though there is some overlap in how the Commission has used the deceptive and unfair rationales, in evaluating the unfairness, the Commission tends to focus on whether or not there is substantial injury to consumers.[9] This commonly includes monetary, health, and safety risks but does not typically include more subjective harms.[10] Within the privacy space, the FTC has found that retroactive changes to a company's privacy policy amount to an unfair act, and it has found the improper use of consumer data to be an unfair practice.[11] The FTC has also previously brought enforcement actions against organizations who have violated consumers' privacy rights under section 5.[12]

B. The Commission Has Authority Under Section 18 to Initiate a Rulemaking with Respect to Unfair Deceptive Acts or Practices

Section 18 of the FTC Act provides the Commission with the authority to adopt "rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce."[13] In order to begin a rulemaking under Section 18, the Commission must have reason to believe the practices to be addressed by the rulemaking are prevalent.[14] The Commission has held workshops, issued reports, conducted investigations, and enforced limited sectoral privacy laws since the 1990s, yet there is still widespread misuse of consumer data.[15]

Today, mobile applications, websites, social media platforms, and smart-devices track your personal information, location, usage data, and contact information and share this information with various third-parties.[16] While the FTC has obtained settlements with Facebook,[17] Flo,[18]

---

[7] *Id.* at 628-633.
[8] *Id.*
[9] *Id.*
[10] *Id* at 638-39.
[11] *Id.* at 639-42.
[12] Federal Trade Commission, "Privacy and Security Enforcement," (last accessed Nov. 14, 2022), https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement.
[13] 15 U.S.C. Sec. 57a
[14] 15 U.S.C. Sec. 57a(b)(3).
[15] Electronic Privacy Information Center, *What the FTC Could Be Doing (but Isn't) to Protect Privacy* (June 2021), https://epic.org/documents/epic-ftc-unused-authorities-report-june2021-2/.
[16] Louise Matsakis, "The WIRED Guide to Your Personal Data (and Who Is Using It), WIRED (Feb. 15, 2019), https://www.wired.com/story/wired-guide-personal-data-collection/.
[17] Lesley Fair, "FTC's $5 Billion Facebook Settlement: Record-Breaking and History-Making," FTC Business Blog (July 24, 2019), https://www.ftc.gov/business-guidance/blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-and-history-making.
[18] Press Release, Federal Trade Commission, FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others (June 22, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google.

Twitter,[19] Weight Watchers,[20] and more, these examples illustrate just a small fraction of the harms that occur on a daily basis. There is little doubt that the prevalence of these practices supports the Commission's position that it has authority under Section 18 to initiate this rulemaking.

C. Existing Inadequacies and Gaps in Industry Self-Regulation and Sector-Specific Regulation Creates the Need for an FTC Rulemaking

Due to existing inadequacies and gaps in industry self-regulation and sector-specific regulation, it is now more important than ever that the FTC develop industry-wide rules to protect consumer data from misuse.

1. Industry self-regulation has failed

The regulation of data privacy practices has largely fallen on the industry itself. This is due to a number of different factors. Previous attempts by the Executive Branch to regulate privacy that have included self-regulatory schemes have been far too deferential to industry, like during the Obama administration when the National Telecommunications and Information Administration worked with various stakeholders in an attempt to develop privacy practices across different industries.[21] The effort failed, as many companies chose not to sign on to the voluntary proposal.[22]

Industry has also attempted to influence legislation at the federal level. In response to the introduction of the American Data Privacy and Protection Act ("ADPPA"), data brokers,[23] major tech companies,[24] and various trade associations began lobbying Congress in an attempt to water-down or kill the bill. While it remains to be seen whether or not the ADPPA will pass out of the House, it is unlikely that big tech's lobbying blitz will slow down any time soon.

---

[19] Lesley Fair, "Twitter to Pay $150 Million Penalty for Allegedly Breaking Its Privacy Promises - Again," FTC Business Blog (May 25, 2022), https://www.ftc.gov/business-guidance/blog/2022/05/twitter-pay-150-million-penalty-allegedly-breaking-its-privacy-promises-again.

[20] Press Release, Federal Trade Commission, FTC Takes Action Against Company Formerly Known as Weight Watchers for Illegally Collecting Kids Sensitive Health Data (Mar. 4, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-company-formerly-known-weight-watchers-illegally-collecting-kids-sensitive.

[21] Natasha Singer, "Why a Push for Online Privacy Is Bogged In Washington," N.Y. Times (Feb. 28, 2016), https://www.nytimes.com/2016/02/29/technology/obamas-effort-on-consumer-privacy-falls-short-critics-say.html.

[22] *Id.*

[23] Alfred Ng, "Privacy Bill Triggers Lobbying Surge by Data Brokers," https://www.politico.com/news/2022/08/28/privacy-bill-triggers-lobbying-surge-by-data-brokers-00052958.

[24] Margaret Harding McGill, "Online Privacy Bill Faces Daunting Roadblocks, Axios (Aug. 4, 2022), https://www.axios.com/2022/08/04/online-privacy-bill-roadblocks-congress.

As a result, the industry has largely been left to self-regulate. Self-regulatory frameworks are often not strong enough to protect consumers, may not get industry-wide participation, and are ineffective because they are unenforceable.[25] They allow these companies to operate in their best interest, not that of consumers. Instead of taking proactive measures to protect consumers, self regulation encourages companies to collect as much data as possible to increase their profits.[26]

2. Sectoral approach leaves significant swaths of consumer data unregulated

The Children's Online Privacy Protection Act ("COPPA"), Gramm-Leach Bliley Act ("GLB"), CAN-SPAM Act, Fair Credit Reporting Act ("FCRA"), Fair Debt Collections Practices Act, and the Telemarketing and Consumer Fraud and Abuse Prevention Act all give the Commission the ability to enforce sector-specific privacy laws.[27] In addition, other federal agencies regulate privacy through sector-specific laws including the Federal Communications Commission,[28] Department of Health and Human Services,[29] and the Consumer Financial Protection Bureau.[30] While sector-specific privacy laws are critical to providing protections for certain types of data and communities,[31] the current approach leaves massive amounts of consumer data unregulated and fails to adequately oversee the data practices of the vast majority of products and services used by people every day.

Although the Commission is able to regulate many of the companies that fall out of the scope of the sectoral laws via the FTC Act, the overwhelming majority of the enforcement actions end in settlements and leave little to no case law.[32] This is in part because the FTC is limited in its ability to seek civil penalties for first-time violations of Section 5, and frequently settles cases instead of taking them to court. Instead of resulting in meaningful change, these settlements typically have little effect on a company's structure or the business incentives around data collection.[33] For example, the investigation into Facebook in the wake of the Cambridge

---

[25] Robert Gellman and Pam Dixon, *Many Failures: A Brief History of Privacy Self-Regulation in the United States*, World Privacy Forum (Oct. 14, 2011), http://www.worldprivacyforum.org/wp-content/uploads/2011/10/WPFselfregulationhistory.pdf

[26] Joe Toscano, "Data Privacy Issues Are the Root of Our big Tech Monopoly Dilemma," Forbes (Dec. 1, 2021), https://www.forbes.com/sites/joetoscano1/2021/12/01/data-privacy-issues-are-the-root-of-our-big-tech-monopoly-dilemma/?sh=7e90de0c3cfd.

[27] Federal Trade Commission, *FTC Report to Congress on Privacy and Security* (Sept. 2021), https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf.

[28] 47 U.S.C. § 222.

[29] 42 U.S.C. § 1320d–2.

[30] 15 U.S.C. § 6803(f).

[31] Commissioner Christine A. Varney, Consumer Privacy in the Information Age: A View from the United States, Address Before the Privacy & American Business National Conference (Oct. 9, 1996), https://www.ftc.gov/news-events/news/speeches/consumer-privacy-information-age-view-united-states.

[32] Solove and Hartzog, *supra* note 6 at 605-06.

[33] Commissioner Rohit Chopra, "Lessons from the FTC's Facebook Saga," The Regulatory Review (Sept. 27, 2022), https://www.theregreview.org/2022/09/27/chopra-lessons-from-the-ftcs-facebook-saga/.

Analytica scandal resulted in a $5 billion fine and did little to change the company's business models and practices.[34] This has left consumers without adequate protection and businesses without a clear understanding of what the law is.[35]

3. State-by-State approach leaves hundreds of millions of consumers unprotected

States are often referred to as laboratories of democracy and over the past four years, five states (California, Colorado, Connecticut, Utah, and Virginia) have enacted comprehensive consumer data privacy laws.[36] Other states, such as Vermont and Nevada, have passed laws to regulate data brokers.[37] While states should certainly exercise their existing authorities to protect user privacy, this approach has left consumers in these states with varying degrees of protection, and consumers in states without data privacy laws with few protections at all. For example, a California resident may be able to sue if their personal information appears in a data breach, while someone in Virginia has to rely on the Attorney General to vindicate their statutory rights.[38]

Lobbying efforts from industry have also watered down state efforts to pass strong privacy legislation. For example, Virginia and Utah's privacy laws were heavily influenced by the companies the bills intended to regulate, and industry has pushed states to pass similar legislation in statehouses across the country.[39]

The varying degrees of protection offered in current state laws combined with industry efforts to pass weaker state laws underscores the need for the FTC to undergo the proposed rulemaking.

---

[34] *Id.*
[35] Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, Council on Foreign Relations (Jan. 30, 2019), https://www.cfr.org/report/reforming-us-approach-data-protection.
[36] National Conference of State Legislatures, "State Laws Related to Digital Privacy," (June 7, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.
[37] *Id.*
[38] Cathay Cosgrove and Sarah Rippy, "Comparison of Comprehensive Data Privacy Laws in Virginia, California, and Colorado," IAPP (July 2021), https://iapp.org/resources/article/comparison-comprehensive-data-privacy-laws-virginia-california-colorado/.
[39] Todd Feathers and Alfred Ng, "Tech Industry Groups Are Watering Down Attempts at Privacy Regulation, One State at a Time," The Markup (May 26, 2022), https://themarkup.org/privacy/2022/05/26/tech-industry-groups-are-watering-down-attempts-at-privacy-regulation-one-state-at-a-time.

III. Online Business Models Incentivize Harmful Commercial Surveillance Practices

Questions one through twelve in the ANPR, ask about the various practices companies use to surveil consumers and protect their data.[40] First, it is important to understand that the business model of many online companies, including major social media platforms, is based on collecting as much personal data on their users as possible to generate profit. Next, online companies can process collected data using algorithms and other artificial intelligence tools to amplify fraudulent content or engage in discriminatory decisionmaking. Finally, many companies share or sell the data they collect to third-party advertisers or data brokers, which can lead to discriminatory forms of ad targeting Each of these business models incentivizes harmful commercial surveillance practices.

A. Commercial Surveillance Business Practices Rely on Pervasive Data Collection

Modern commercial surveillance practices rely heavily on mass data collection. The average consumer spends over four hours a day online, and the data collected by the various platforms, websites, and devices they use is the currency that fuels the digital economy. [41] How this data is collected and what it is used for varies, but all of these businesses frequently gather massive amounts of sensitive and non-sensitive consumer data, often without the user's consent.[42] Everything from credit card data to health information is collected,[43] and many companies collect information on users' race and gender identity or information that can be used as a proxy for a user's race and gender.[44] It has been estimated that by the time a child is thirteen, online advertising firms have collected on average 72 million data points about them.[45] Google knows everywhere someone has been since the day they downloaded Google on their phone and much more.[46] Consumers have so much data collected about them, and the practice is so widespread,

---

[40] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273 (proposed Aug. 22, 2022).
[41] Justin Brockman, *Understand the Scope of Data Collection by Major Technology Platforms,* Consumer Reports (May 2020), https://digital-lab.consumerreports.org/wp-content/uploads/2021/02/Understanding-the-scope-of-data-collection-by-major-platforms_2020_FINAL.pdf.
[42] *Id.*
[43] *Id.*
[44] Becky Chao, et al., *Centering Civil Rights in the Privacy Debate,* Open Technology Institute (Aug. 2019), https://www.newamerica.org/oti/reports/centering-civil-rights-privacy-debate/for-marginalized-communities-the-stakes-are-high.
[45] Dave Davies, "Users Beware: Apps Are Asing a Looping in Privacy Law To Track Kids' Phones," NPR (June 16, 2022), https://www.npr.org/2022/06/16/1105212701/users-beware-apps-are-using-a-loophole-in-privacy-law-to-track-kids-phones.
[46] Dylan Curran, "Are You Ready? Here is All the Data Facebook and Google Have on You," The Guardian (Mar. 30, 2018), https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy.

that most Americans feel they have no control over the data companies collect and believe that the potential risks of companies collecting data outweigh the benefits.[47]

B. Algorithmic Tools Can Encourage Fradulent Content or Lead to Discriminatory Decision-Making

As a result of mass data collection practices, many companies are able to deploy algorithms that determine what content users see or what services they can access.[48] Algorithms track user preferences through clicks, 'likes,' 'shares,' and other forms of engagement.[49] Many companies optimize algorithms to maximize user engagement in order to increase revenue.[50] As a result, algorithms, particularly on social media platforms, elevate sensational, eye-catching, and controversial content.[51] Facebook even admitted in an internal memo that the "core product mechanics" had allowed hate speech and misinformation to flourish on the platform.[52] The consequences of this are two-fold. Platforms are both incentivized to leave up otherwise harmful and violative content so that they can continue to increase engagement on their platforms, and to promote this content to users that are most likely to engage with this content.[53] As the Commission has pointed out, these platforms are a "gold mine" for fraud, where bad actors can use the tools available to push false claims about COVID-19.[54] Due to a lack of transparency by the platforms, policymakers and regulators are unable to gain insight into how these algorithmic systems work and address the problems created by these negative incentives.[55]

Companies can also use algorithms to perpetuate existing inequalities through discriminatory decisionmaking. As discussed in greater detail in subsequent sections, automated decisionmaking

---

[47] Brooke Auxier, et al., "Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information," Pew Research Center (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[48] Joanna Stern, "Social-Media Algorithms Rule How We See the World. Good Luck Trying to Stop Them.," Wall Street Journal (Jan. 17, 2021), https://www.wsj.com/articles/social-media-algorithms-rule-how-we-see-the-world-good-luck-trying-to-stop-them-11610884800.

[49] *Id.*

[50] *Id.*

[51] Nathalie Marechal, Rebecca MacKinnon, and Jessica Dheere, *Getting to the Source of Infodemics: Its the Business Model*, Ranking Digital Rights (May 27, 2020), https://www.newamerica.org/oti/reports/getting-to-the-source-of-infodemics-its-the-business-model/.

[52] Dan Milmo and David Pegg, "Facebook Admits Site Appears Hardwired for Misinformation, Memo Reveals," The Guardian (Oct. 25, 2021), https://www.theguardian.com/technology/2021/oct/25/facebook-admits-site-appears-hardwired-misinformation-memo-reveals.

[53] Marechal, MacKinnon, and Dheere, *supra* note 51.

[54] Samuel Levine, "FTC Analysis Shows COVID Fraud Thriving on Social Media Platforms," Federal Trade Commission (Nov. 18, 2021), https://www.ftc.gov/business-guidance/blog/2021/11/ftc-analysis-shows-covid-fraud-thriving-social-media-platforms.

[55] Marechal, MacKinnon, and Dheere, *supra* note 51.

systems have led to discrimination in housing, employment, credit, education, finance, and other economic opportunities.

C. Companies Can Use Data To Engage in Discriminatory Ad Targeting

Companies use massive amounts of data in a couple different ways, one of which is by selling targeted advertisements and offering other businesses commercial algorithmic profiling, targeting, and advertising services.[56] Facebook's ad targeting services offer a perfect case study of why targeted advertising (and the data collection that fuels it) can be extremely harmful. Up until 2020, advertisers were able to use Facebook to target users whom the platform categorized as "African American (US)," "Asian American (US)," or "Hispanic (US-All)."[57] This practice changed after litigation and a civil rights audit, but advertisers can still take advantage of Facebook's Lookalike Audiences and Special Ad Audiences to reach specific demographic groups.[58] So, while Facebook will no longer let advertisers directly target consumers based on demographic characteristics, it does allow advertisers to target consumers "who have expressed an interest in or like pages related to African-American culture."[59] Once an advertiser has picked a characteristic by which to target consumers, Facebook then decides which consumers actually see an ad.[60] This is functionally the same thing as targeting specific demographic groups, and enables both advertisers and Facebook to perpetuate discrimination in housing, credit, and employment.[61] Further, even harmless decisions by advertisers may still be used by Facebook's algorithm in a way that discriminates against marginalized groups.[62] In sharp contrast to harmless decisions by legitimate businesses, bad actors can use the tools available to advertisers to target consumers with "bogus" ads based on personal information.[63]

IV. Commercial Surveillance Generates Harms to Democracy and Civil Rights

Commercial surveillance and data security harms have had a profound impact on our society and the democratic institutions that hold our country together. The Commission asks about these harms throughout the ANPR. For example, question six asks about harms that consumers may not be able to quantify, while question sixty-five asks about the prevalence of algorithmic

---

[56] Tanya Kant, "Identity, Advertising, and Algorithmic Targeting: Or How (Not) to Target Your 'Ideal User,'" MIT Schwartzman College of Computing (Sept. 2, 2021), https://mit-serc.pubpub.org/pub/identity-advertising-and-algorithmic-targeting/release/2.

[57] Jinyan Zang, *Solving the Problem of Racially Discriminatory Advertising on Facebook,* Brookings (Oct. 19, 2021), https://www.brookings.edu/research/solving-the-problem-of-racially-discriminatory-advertising-on-facebook/.

[58] *Id.*

[59] *Id.*

[60] Aaron Rieke and Corrine Yu, "Discrimination's Digital Frontier," The Atlantic (Apr. 15, 2019), https://www.theatlantic.com/ideas/archive/2019/04/facebook-targeted-marketing-perpetuates-discrimination/587059/

[61] *Id.*

[62] *Id.*

[63] Emma Fletcher, "Social Media a Gold Mine for Scammers in 2021," Federal Trade Commission (Jan. 25, 2022), https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/01/social-media-gold-mine-scammers-2022

discrimination.[64] The harms discussed below are not always easy for consumers to identify or measure, but they must be addressed by the Commission in this rulemaking.

A. Democracy Harms

Political campaigns and bad actors are increasingly using online tactics by exploiting data-driven business models to cause great harm to our democracy. Voter suppression and increased threats of physical violence are both the result of an increased ability to obtain comprehensive data on millions of people, reach and influence them in a way unimaginable twenty years ago, and organize radical movements.

1. Pervasive Fraud Online and the Use of Discriminatory Algorithms Enables Voter Suppression

In 2018, most Americans became aware of how online fraud could impact our democracy after news broke that Cambridge Analytica, a political consulting firm, had partnered with researchers to improperly harvest the data profiles of over 80 million people on behalf of Donald Trump and Ted Cruz's political campaigns.[65] Cambridge Analytica, working with SCL Group, had created a web app that required users to consent to giving the app access to their and their friends' Facebook profiles before taking a quiz.[66] This data was then used to build psychological profiles of millions more people and target them.[67]

The following year, the FTC brought and settled an action against Cambridge Analytica, charging them with using trade practices that prevented consumers from "effectively making their own decisions" and causing substantial injury under the deceptive acts or practices prong of Section 5 of the FTC Act.[68] In a related action, the FTC brought and settled an action against Facebook for violating a 2012 order by deceiving users about their ability to control the privacy of their personal information.[69]

---

[64] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273 (proposed Aug. 22, 2022).
[65] Andrew Prokop, "Cambridge Analytica Shutting Down: The Firm's Many Scandal's, Explained," Vox (May 2, 2018), https://www.vox.com/policy-and-politics/2018/3/21/17141428/cambridge-analytica-trump-russia-mueller.
[66] *Id.*
[67] Carole Cadwalldr, "'I Made Steve Bannon's Psychological Warfare Tool': Meet the Data War Whistleblower," The Guardian (Mar. 18, 2018), https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump.
[68] Press Release, Federal Trade Commission, FTC Issues Opinion and Order Against Cambridge Analytica for Deceiving Consumers About the Collection of Facebook Data, Compliance with EU-U.S. Privacy Shield (Dec. 6, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/12/ftc-issues-opinion-order-against-cambridge-analytica-deceiving-consumers-about-collection-facebook.
[69] Press Release, Federal Trade Commission, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019),

While the settlements with Cambridge Analytica and Facebook were a step forward in protecting consumer privacy, Cambridge Analytica was far from the only bad actor in the space and Facebook's conduct has not changed dramatically since the settlement. Just as a private business may choose to target specific demographic groups for advertisements, a political campaign or political action committee may do the same.[70] These campaigns are able to take advantage of the massive amounts of data collected about individuals and purchase political ads with intentionally misleading messages about the time/place/manner in which voting takes place or with messages intended to discourage people from voting.[71] For example, Donald Trump's 2016 presidential campaign labeled 3.5 million Black Americans as 'Deterrence' voters, who the campaign wanted to stay home on election day, and showed them negative videos intended to reduce Democratic turnout.[72]

A recent investigation detailed the dozens of major data brokers that sell voter location data to political campaigns, how they acquire that data, and the other services they offer.[73] These firms provide information on everything from a consumer's credit score to their news consumption habits, and then cross-reference these data points with location data.[74] One firm used this data to help campaigns target voters who were waiting in line to vote at polling locations.[75]

The kind of activity described above is deeply harmful to our democracy and unduly undermines peoples' choices.[76] Consumers targeted by voter suppression campaigns may not fully understand the extent to which the campaigns targeting them have their data or the manner in

---

https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook.

[70] Zang, *supra* note 57.

[71] Ciara Torres-Spelliscy, "A Lie Just for You in 2022," Brennan Center for Justice (Sept. 21, 2020), https://www.brennancenter.org/our-work/analysis-opinion/lie-just-you-2020.

[72] Channel 4 News Investigations Team, "Revealed: Trump Campaign Strategy to Deter Millions of Black Americans from Voting in 2016," Channel 4 News (Sept. 28, 2020), https://www.channel4.com/news/revealed-trump-campaign-strategy-to-deter-millions-of-black-americans-from-voting-in-2016; *See also* Derek Hawkins, "No, You Can't Text Your Vote. But These Fake Ads Tell Clinton Supporters To Do Just That," Washington Post (Nov. 3, 2016), https://www.washingtonpost.com/news/morning-mix/wp/2016/11/03/no-you-cant-text-your-vote-but-these-ads-tell-clinton-supporters-to-do-just-that/ (discussing fake ads aimed at Black and Latino voters telling them they can text their vote for Hillary Clinton); Michelle Castillo, "Facebook Was Manipulated by Russians, Who Used the Same Targeting Tools That Advertisers Love," CNBC (Dec. 17, 2018), https://www.cnbc.com/2018/12/17/facebook-ad-platform-made-it-easy-for-russians-to-manipulate-users.html (discussing a Senate Intelligence Committee report showing Russia's Internet Research Agency bought ads intending to sway and misinform U.S. voters).

[73] Jon Keegan, " How Political Campaigns Use Your Phone's Location to Target You," The Markup (Nov. 8, 2022), https://themarkup.org/privacy/2022/11/08/how-political-campaigns-use-your-phones-location-to-target-you.

[74] *Id.*

[75] *Id.*

[76] Danielle Keats Citron and Daniel J. Solove, *Privacy Harms*, 102 Boston University L. Rev. 793, 845-49 (2022), https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf.

which the third-party is attempting to influence their decision making process.[77] While the Commission has not explicitly found this specific kind of practice to be unfair or deceptive, it has stated that trade practices that prevent consumers from "effectively making their own decisions" are ones that cause substantial injury,[78] and given the scale at which this practice is used, and will likely continue to be used, it should be considered reasonably unavoidable by consumers.

2. The Algorithmic Amplification of Fraudulent Content Can Lead to Physical Harm and Offline Violence

In addition to broader democracy harms, privacy violations can also result in physical harm and offline violence. When personal data is shared improperly, it creates a unique opportunity for violence.[79] In advance of the January 6th insurrection, platform algorithms amplified content from the "Stop the Steal" movement. Tens of thousands of users joined "Stop the Steal" affiliated groups every hour, as Facebook's algorithm allowed for the mass sending of invites and even suggested that users with certain interests join these groups.[80] These groups worked in tandem to coordinate the January 6th insurrection, and in an internal memo Facebook recognized the role its platform played in causing it.[81] Even the algorithms used by businesses encouraged violence, as a report found that Facebook showed ads for military gear next to posts about the January 6th insurrection.[82]

B. Civil Rights Harms

The prevalence of civil rights harms that stem from commercial surveillance and data practices are well documented. Numerous lawsuits addressing the impact of discriminatory advertising and data usage have been brought by the American Civil Liberties Union ("ACLU") and the U.S. Department of Justice ("DOJ"), among others.[83] In both the ACLU and DOJ's lawsuits,

---

[77] *Id.*
[78] *Id.*
[79] *Id*. at 831-33.
[80] Shannon Bond and Bobby Allyn, "How the Stop the Steal Movement Outwitted Facebook Ahead of the Jan. 6 Insurrection," NPR (Oct. 22, 2021), https://www.npr.org/2021/10/22/1048543513/facebook-groups-jan-6-insurrection.
[81] *Id.*
[82] Ryan Mac and Craig Silverman, "Facebook Has Been Showing Military Gears Ads Next to Insurrection Posts," BuzzFeed News (Jan. 13, 2021), https://www.buzzfeednews.com/article/ryanmac/facebook-profits-military-gear-ads-capitol-riot.
[83] Galen Sherwin and Esha Bhandari, "Facebook Settles Civil Rights Cases by Making Sweeping Changes to Its Online Ad Platform," American Civil Liberties Union (Mar. 2019), https://www.aclu.org/news/womens-rights/facebook-settles-civil-rights-cases-making-sweeping; Press Release, U.S. Department of Justice, Justice Department Secures Groundbreaking Settlement Agreement with Meta Platforms, Formerly Known as Facebook, to Resolve Allegations of Discriminatory Advertising (June 21, 2022), https://www.justice.gov/opa/pr/justice-department-secures-groundbreaking-settlement-agreement-meta-platforms-formerly-known.

Facebook, as part of the settlements, had to make changes to its advertising system, which plaintiffs claimed discriminated against members of protected classes in the targeting of employment and housing ads, respectively.[84] Unfortunately, these cases represent just a small fraction of the algorithmic discrimination that occurs online on a regular basis and do not begin to mitigate the harms caused by these practices.

1. Pervasive Algorithmic Discrimination Negatively Impacts the Ability of Marginalized Communities to Fully Participate in Society by Entrenching Inequality

When businesses and institutions are able to take advantage of big data to discriminate (intentionally or unintentionally) based on protected characteristics, it further entrenches existing inequalities and disadvantages marginalized communities. Opaque algorithms have been found to reproduce patterns of discrimination in employment,[85] housing,[86] education,[87] mortgage lending,[88] credit scoring,[89] and other areas critical to full participation in society.[90] While there are laws in place that are intended to prevent discrimination in these areas, bias creeps into these algorithms through the data sets used to power them.[91]

Discrimination in each of these areas compounds. For example, researchers have found that the credit scores of Black and white Americans differ significantly.[92] A lower credit score then

---

[84] Galen Sherwin and Esha Bhandari, "Facebook Settles Civil Rights Cases by Making Sweeping Changes to Its Online Ad Platform," American Civil Liberties Union (Mar. 2019), https://www.aclu.org/news/womens-rights/facebook-settles-civil-rights-cases-making-sweeping; Press Release, U.S. Department of Justice, Justice Department Secures Groundbreaking Settlement Agreement with Meta Platforms, Formerly Known as Facebook, to Resolve Allegations of Discriminatory Advertising (June 21, 2022), https://www.justice.gov/opa/pr/justice-department-secures-groundbreaking-settlement-agreement-meta-platforms-formerly-known.

[85] Miranda Bogen and Aaron Rieke, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias*, UpTurn (Dec. 2018), https://www.upturn.org/static/reports/2018/hiring-algorithms/files/Upturn%20--%20Help%20Wanted%20-%20An%20Exploration%20of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf.

[86] Valerie Schneider, *Locked Out by Big Data: How Big Data, Algorithms, and Machine Learning May Undermine Housing Justice*, 52 Columbia L. Rev 252 (2020), https://blogs.law.columbia.edu/hrlr/files/2020/11/251_Schneider.pdf.

[87] Hannah Quay-de la Vallee and Natasha Duerte, *Algorithmic Systems in Education: Incorporating Equity and Fairness When Using Student Data*, Center for Democracy and Technology (Aug. 2019), https://cdt.org/wp-content/uploads/2019/08/2019-08-08-Digital-Decision-making-Brief-FINAL.pdf.

[88] Diana Olick, "A Troubling Tale of a Black Man Trying to Refinance his Mortgage," CNBC (Aug. 19, 2020), https://www.cnbc.com/2020/08/19/lenders-deny-mortgages-for-blacks-at-a-rate-80percent-higher-than-whites.html.

[89] Lisa Rice and Deidre Swesnik, *Discriminatory Effects of Credit Scoring on Communities of Color,* 46 Suffolk Univ. L. Rev. 935 (2013), https://cpb-us-e1.wpmucdn.com/sites.suffolk.edu/dist/3/1172/files/2014/01/Rice-Swesnik_Lead.pdf.

[90] Yashimabeit Milner and Amy Taub, *Data Capitalism and Algorithmic Racism,* Demos (2021), https://www.demos.org/sites/default/files/2021-05/Demos_%20D4BL_Data_Capitalism_Algorithmic_Racism.pdf.

[91] Adam Zewe, "Fighting Discrimination in Mortgage Lending," MIT News (Mar. 30, 2022), https://news.mit.edu/2022/machine-learning-model-discrimination-lending-0330.

[92] Milner and Taub, *supra* note 90.

makes it more difficult to secure a loan for a house, and when algorithms determine that even with a high credit score a Black person is not qualified the process becomes significantly more difficult.[93] Many of these practices would be violations of Federal and state civil rights law if carried out by an individual or group of individuals instead of algorithms, but these laws have not been adequately applied to privacy violations.[94]

The harms stem from practices that are inherently both unfair and deceptive. Discrimination carries more than just harm to any one individual, it has a systemic affect on the communities it impacts and broader societal effects.[95] There is not one simple way to categorize the harms that stem from discrimination. Someone may be denied an equal chance to obtain employment or find housing while another may face online harassment and exposure to physical violence.[96]

Many of these algorithms are unavoidable for consumers. Regulatory action is taken by the Commission where "there is an obstacle to the free exercise of consumer decision making,"[97] and when a consumer faces bias from algorithms in areas like housing and employment that are so critical to participating in society, these algorithms present a real obstacle to the free exercise of their decision making.

Although data collection and micro-targeting certainly benefit many businesses, the harms to marginalized groups and the entrenchment of inequality based on gender, race, national origin, sexual orientation, and age warrant action to be taken by the Commission.

V. The Commission Should Adopt A Comprehensive Set of Rules to Address Commercial Surveillance Harms

There are a number of different rules the Commission should adopt to address the problems discussed in this comment as outlined below.

A. Data Minimization Framework

One way the Commission can begin to regulate the widespread collection of consumer data is by limiting the types of data companies can collect and sell. Apps and websites frequently collect data they do not need or even use, and currently only need consumer consent to do so.[98] A data

[93] Diana Olick, "A Troubling Tale of a Black Man Trying to Refinance His Mortgage," CNBC (Aug. 19, 2020), https://www.cnbc.com/2020/08/19/lenders-deny-mortgages-for-blacks-at-a-rate-80percent-higher-than-whites.html.
[94] Citron and Solove, *supra* note 76 at 845-49.
[95] Citron and Solove, *supra* note 76 at 855.
[96] Citron and Solove, *supra* note 76 at 855-57.
[97] Dennis D. Hirsch, *That's Unfair! Or Is It? Big Data, Discrimination, and the FTC's Unfairness Authority,* 103 U. Ky. L. Rev. 345, 353 (2015), https://uknowledge.uky.edu/cgi/viewcontent.cgi?article=1073&context=klj.
[98] Kaveh Waddell, "Some Developers Don't Know What Their Apps Do With Your Data," Consumer Reports (Mar. 13, 2020), https://www.consumerreports.org/privacy/developers-dont-know-what-their-apps-do-with-your-data-a1055672912/.

minimization rule would require businesses to collect, use, and disclose data only as reasonably necessary to provide the service requested by the consumer.[99] Consumer Reports and Epic have suggested three different ways this can be accomplished: by prohibiting all secondary data uses with limited exceptions; prohibiting specific secondary data uses; or mandating a right to opt out of secondary data use.[100] In contrast with the current "notice and choice regime," a data minimization rule would reduce the risk of consumer exposure to data breaches, employee misuses, unwanted secondary uses, and inappropriate government access.[101]

B. Nondiscrimination Rules and Civil Rights Protections

There are two different sets of nondiscrimination rules the Commission must implement during this rulemaking. The first involves rules that prevent companies from discriminating against consumers who choose to exercise their privacy rights.[102] Today, consumers can pay higher fees to avoid data collection and targeted advertising while consumers who agree to certain companies' data collection practices can receive a discount on their services.[103] This has created a scheme where privacy is not a right - it's a luxury. Rules promulgated by the Commission must change this, and make clear that privacy is a fundamental right for everyone, regardless of income.[104]

The second rule should adopt robust civil rights protections that prohibit data-driven discrimination and ensures everyone has the right to equal opportunity online.[105] The Commission should use the ADPPA as a model for developing rules to protect civil rights on the internet.

C. Individual Rights

Every state privacy law currently on the books gives consumers the right to access, correct, and delete personal data and the ability to opt out of the processing of personal data.[106] These rights, while not sufficient on their own, should be available to every consumer in the country. Doing so

---

[99] Consumer Reports and Electronic Privacy Information Center, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking* (Jan 26. 2022), https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf.
[100] *Id.*
[101] *Id.*
[102] *Id.*
[103] Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy,* 117 Columbia L. Rev. 1369, 1373 (2017), https://columbialawreview.org/content/paying-for-privacy-and-the-personal-data-economy/.
[104] Consumer Reports and Electronic Privacy Information Center, *supra* note 99.
[105] *Id.*
[106] National Conference of State Legislatures, "State Laws Related to Digital Privacy," (June 7, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

will empower consumers, allowing them to have greater control over their own personal information.

D. Transparency

Any rules created by the Commission must include some transparency requirements for both the primary and secondary uses of data, as well as requirements around the algorithms used to place ads. Transparency rules should promote accountability and empower consumers to make decisions about who and when they provide access to their data.[107] This could mean labeling requirements for specific transactions, mandating more easily understood privacy policies, or documentation requirements for certain types of data process.[108] Regarding algorithms, the Commission could require the disclosure of policies that govern the use of certain algorithms and how they impact the user experience.[109]

VI. Conclusion

This rulemaking represents a tremendous opportunity to mitigate certain commercial surveillance practices that have led to a number of harms. The recommendations discussed above encourage the FTC to adopt a comprehensive regulatory approach that would give individuals far greater control over their data, safeguard civil rights online, and ensure bad actors cannot exploit data to undermine our democracy. We thank the FTC for its work in this vital area and encourage its thoughtful consideration of these comments.

Respectfully submitted,
/s/ Jonathan Walter
/s/ Yosef Getachew
Common Cause
805 15th St. NW,
Suite 800
Washington, D.C. 20005

November 21, 2022

[107] Consumer Reports and Electronic Privacy Information Center, *supra* note 99.
[108] *Id*.
[109] Spandana Singh, *Regulating Platform Algorithms: Approaches for EU and U.S. Policy Makers,* Open Technology Institute (Dec. 1, 2021), https://www.newamerica.org/oti/briefs/regulating-platform-algorithms/.