Before the
FEDERAL TRADE COMMISSION
Washington, D.C. 20024

In the Matter of	)	
	)	
	)	
Commercial Surveillance	)	ANPR R111004
	)	
	)	

COMMENTS OF NEXT CENTURY CITIES

Ryan Johnston
Senior Policy Counsel

Roxanna Barboza
Program Director

November 18, 2022

Table of Contents

Before the
FEDERAL TRADE COMMISSION
Washington, D.C. 20024

In the Matter of	)	
	)	
	)	
Commercial Surveillance	)	ANPR R111004
	)	
	)	

COMMENTS OF NEXT CENTURY CITIES

I. Introduction

Next Century Cities ("NCC")[1] submits these comments in response to the Federal Trade Commission's Advanced Notice of Proposed Rulemaking on Commercial Surveillance and Data Security ("ANPRM").[2] Both the Federal Communications Commission and National Telecommunications and Information Administration are working diligently to increase the access and adoption rates of broadband nationwide. As federal, state, and local governments work in tandem to make high-speed Internet connectivity ubiquitous, the Federal Trade Commission ("FTC" or "Commission") should do more to protect users' data privacy.

The large volume of user data that online surveillance generates coupled with historically inadequate data security practices has increased the danger that consumers face online. Individuals are more likely than ever to fall victim to error, deception, or abuse of data generated online. The FTC is best positioned to investigate how commercial surveillance and data practices

[1] Next Century Cities is a nonprofit nonpartisan 501(c)(3) coalition of over 250 member municipalities that work collaboratively with local leaders to ensure reliable and affordable broadband access for every resident in every community.
[2] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51, 273 (Aug. 22, 2022).

impact consumer privacy. Moreover, it has the requisite authority to promulgate new rules that help shield consumers from deceptive practices in ways that also deters corporate misconduct.

II. Lax Data Security Practices Invite Consumer Harms.

One need not look past the headlines on a given week to see that a corporation has mishandled consumer information or had a data breach that has put consumers' data at risk.[3] Businesses generally collect four types of data that allow them to build comprehensive profiles of the consumers that use their goods and services: personal, engagement, behavioral, and attitudinal data.[4] This data gives businesses clear insights into the demographic information, interests, transactional details, and potential needs of the consumers they serve.

The potential for significant consumer harm is not unknown. Recently, the Consumer Financial Protection Bureau ("CFPB") released Circular 2022-04, which reaffirmed that entities can violate the Consumer Financial Protection Act's prohibition on unfair acts or practices when they fail to impose sufficient data protection or information security practices to protect consumer data.[5] The CFPB concluded that inadequate data security measures can cause significant harm, or a risk of harm, to consumers even in the absence of an actual data breach.[6] Consumers cannot avoid the fallout from data security failures as they have no way of knowing whether security measures are properly implemented and they lack the practical means to avoid harm.[7]

---

[3] Michael X. Heiligenstein, *Recent Data Breaches*, Firewall Times (Oct. 3, 2022), https://firewalltimes.com/recent-data-breaches/.
[4] Max Freedman, *How Businesses are Collecting Data (And What They're Doing With It)*, Business News Daily (Aug. 25, 2022), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html.
[5] Consumer Financial Protection Bureau, Consumer Financial Protection Circular 2022-04, https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/ (last visited Oct. 13, 2021).
[6] *Id.*
[7] *Id.*

The FTC should take a similar stance and extend the application of its proscription on "unfair or deceptive business practices" to inadequate data security for information collected, processed, maintained, or stored by a company. That posture would require companies to put risk mitigation measures in place. Additionally, the FTC should require businesses to take stock of the information it collects, how data is stored, and protocols used to obtain consumer consent. Taking a stance similar to the CFPB's would signal to businesses that the Commission is intent on addressing lax data security practices with every tool at its disposal.

Inevitably, harms will arise from the automated processes that businesses use to collect and share consumer data. Particularly in these instances, ensuring that data management protocols are audited for discriminatory impact is essential.

III. Discriminatory Data Collection Practices Have Wide-Reaching Effects.

Commercial data collection practices allow businesses to collect and monetize data at a massive scale with little scrutiny or limitation. Likewise, commercial surveillance practices have enabled discriminatory advertising, racially biased policing, and the outing or surveillance of historically marginalized groups.[8] Algorithms that are designed or implemented poorly can perpetuate biases in housing, employment, and banking ads. For example, in 2015, a study from Carnegie Mellon University showed that men browsing job listing sites were more likely to be

[8] Samantha Lai and Brooke Tanner, *Examining the intersection of data privacy and civil rights*, Brookings (July 18, 2022), https://www.brookings.edu/blog/techtank/2022/07/18/examining-the-intersection-of-data-privacy-and-civil-rights/.

shown ads with higher salaries than women.[9] Similarly, ProPublica found, in 2018, that many Facebook ads for Uber were not visible to women.[10]

Discriminatory data management protocols also have a measurable impact on housing. A study from the University of California at Berkeley found that online lenders offered higher interest rates to African Americans and Latinos based on data collected on user behavior and location.[11] In 2019, Meta settled a case with the U.S. Department of Housing and Urban Development over the company not displaying housing ads to people based on protected characteristics, including race.[12] Housing, much like gender and race-based discrimination in job postings, persists in the targeting of housing ads even when advertisers do not opt to target specific demographics.[13]

Discriminatory data practices also continue, and can worsen inequalities in socioeconomic status.[14] Companies use consumer-generated data to "personalize" prices and products for those living in specific neighborhoods.[15] As such, people living in wealthier neighborhoods may have access to better prices or products than someone living in a poorer

[9] Caroline Leopold, *Google algorithms show higher paying jobs to more men than women*, Digital Journal (July 8, 2015), https://www.digitaljournal.com/social-media/google-algorithms-show-higher-paying-jobs-to-more-men-than-women/article/437802#ixzz7hdCRKAKA.
[10] Ariana Tobin and Jeremy B. Merrill, *Facebook Is Letting Job Advertisers Target Only Men*, ProPublica (Sept. 18, 2018), https://www.propublica.org/article/facebook-is-letting-job-advertisers-target-only-men.
[11] Laura Counts, *Minority homebuyers face widespread statistical lending discrimination, study finds*, BerkeleyHaas (Nov. 3, 2018), https://newsroom.haas.berkeley.edu/minority-homebuyers-face-widespread-statistical-lending-discrimination-study-finds/.
[12] Linda Morris and Olga Akselrod, *Holding Facebook Accountable for Digital Redlining*, ACLU (Jan. 27, 2022), https://www.aclu.org/news/privacy-technology/holding-facebook-accountable-for-digital-redlining.
[13] Muhammad Ali et al., *Discrimination through optimization: How Facebook's ad delivery can lead to skewed outcomes*, Cornell University (Sept. 12, 2019), https://arxiv.org/abs/1904.02095.
[14] Becky Chao et al., *Centering Civil Rights in the Privacy Debate*, Open Technology Institute at New America (Aug. 14, 2019), https://www.newamerica.org/oti/reports/centering-civil-rights-privacy-debate/#authors.
[15] *Id*.

one.[16] Data that is originally collected with good intentions can easily be repurposed to discriminate or exclude minorities and disadvantaged communities.[17]

Regardless of intent, algorithmic discrimination in all its forms is detrimental to consumers. The Commission should evaluate and restrict these types under its unfair and deceptive practices definitions. Left unchecked, algorithmic discrimination will become an industry standard. The breadth of well-documented harms warrants federal safeguards that help eliminate predatory and discriminatory practices online.

IV. Clear and Transparent Surveillance and Data Collection Policies Are Essential for Effective Consumer Consent.

Questions posed in the ANPRM provide useful starting points for coordination and administration of consumer transparency and consent practices. NCC recommends, however, that new processes should go beyond historical practices, and put consumer perspectives at the forefront of the FTC's evaluation process. Also, as a background note, getting this right should be seen as a top priority for the Commission and businesses alike. Consumers support the government taking a leading role in protecting privacy.[18] They depend on the Commission to set standards for – and enforce – a consumer's right to privacy.

NCC urges the FTC to incorporate the following recommendations into any framework used to evaluate a company's commercial surveillance and data security practices.

1. The FTC can help to ensure that consumers understand what they agree to by developing universal guidance on data management and consumer consent policies. This guidance

[16] *Id.*
[17] *Id.*
[18] Data Transparency's Essential Role in Building Customer Trust, CISCO (2022), https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-survey-2022.pdf?CCID=cc000160&DTID=esootr000875&OID=wprsc030156.

should be formatted in a way that is categorized into different subjects and is easy to comprehend when companies are asking for data management consent. At a minimum, categories must address how consumer data is collected, stored, shared, and monetized.

2. Audit a company's consumer consent processes on an annual basis. Annual reviews would enable the FTC to monitor whether companies are appropriately using consumer's data and providing consumers with appropriate notice of changes. Given that businesses range in size, the Commission should identify appropriate benchmarks policies for businesses of varying sizes. Effective implementation and enforcement could reduce future harms by setting new standards for emerging companies that engage in commercial surveillance and brokering data.
3. The FTC should develop a framework for businesses that outlines safe data collection procedures. Doing so would help to standardize methods for large-scale data collection, processing, and storage. The Commission has an important role to play in helping to eliminate loopholes for predatory data collection and use. Consumer safeguards would also help to ensure that new and existing consumers ultimately benefit from getting online. Importantly, local and state governments that are working to develop new networks – or upgrading outdated – digital infrastructure would also benefit from learning about best practices for handling their constituents' data.
4. Develop protocols for secure data management that minimizes cybersecurity concerns. Chiefly, the FTC must develop rules and provide educational materials on tested data protection protocols. It should also share best practices for consumers to learn how to avoid online threats.

5. The FTC should consider building a database in which consumers are able to search where and how their data is being collected and if personally identifiable information (name, address, etc.) is being traded online. The database should disclose how businesses that are registered with the Commission claim they are collecting and using consumers' data. A public database would facilitate consumers' ability to identify and request the deletion of personal information. It would also enable consumers to opt-out of the sale of their personal information.
6. Establish an advisory committee to guide the FTC on the recommendations listed above. Advisory committee recommendations could be used to inform future updates to FTC rules. Members should be representative of consumer advocacy groups, state and local governments, small businesses, and large corporations, with no more than one-third representing industry stakeholders. The advisory committee should meet on a semi-annual basis for no more than a two-year term.

These measures would incorporate essential perspectives into FTC data privacy policies.

V. The Commission Must Commence a Section 18 Rulemaking to Adequately Address Surveillance and Data Collection Concerns.

In the past, the Commission has utilized its Section 5 unfair and deceptive practices authority to address a variety of harmful practices, including failures to reasonably secure personal information.[19] The Commission has also wielded this authority to address the selling of sensitive data[20] and the sale of data without the notice and consent from the individual.[21] Since 2020, the FTC has brought twenty lawsuits against organizations that have violated consumers'

[19] *See* e.g. *In the Matter of InfoTrax Systems, L.C.*, FTC File No. 162 3130, Docket No. C-4696 (2019); *FTC v. Equifax,* No. 1:19-cv-03927- TWT (N.D. Ga. 2019).
[20] *FTC v. Sitesearch Corp. d/b/a LeapLab*, No. 2:14-cv-02750 (D. Ariz. Feb. 18, 2016).
[21] *FTC v. Vizio, Inc.*, No. 2:17-cv-00758 (D.N.J. 2017).

privacy rights, misled them by failing to maintain security for sensitive information, or caused substantial consumer injury.

Section 18 of the FTC Act authorizes the Commission to prescribe rules "which define with specificity acts or practices which are unfair or deceptive acts or practices. . . ."[22] The Commission may initiate a Section 18 rulemaking when it has reason to believe that practices to be addressed by the rulemaking are "prevalent."[23] Through the ANPRM, the Commission has identified over 90 specific areas where a failure to secure personal information or to protect the privacy interests of consumers could be considered unfair or deceptive. Many of the practices outlined in the ANPRM have already been addressed by the Commission, which sets a precedent that these practices are unfair or deceptive.

A section 18 rulemaking will give the Commission the greatest amount of latitude to hear from interested parties and experts, collect evidence, address advances in technology, and fold in new protections as necessary. As states continue to work on their own sets of privacy laws and regulations, in-depth federal rulemaking should provide a floor for states that are interested in taking their own actions.

Further, a new FTC rulemaking could also spur Congress to pass much-needed federal privacy legislation. Such a significant undertaking by the Commission will bring a dearth of relevant information to the forefront of policy discussions. The FTC should not keep trying to avoid creating a comprehensive set of final rules protecting consumers. At the very least, the Commission should bring experts and policy discussions to the forefront and provide an untold amount of meaningful material to those who are working on drafting state and federal privacy legislation.

[22] 15 U.S.C. § 57a(a).
[23] *Id.*

Finally, the Commission should create a bureau within the Federal Trade Commission dedicated to handling Internet-related policymaking and enforcement. For over 100 years, the Commission has presided over consumer protection measures and competition policy across industries ranging from home appliances to clothing and textiles. Housing Internet-related policy and enforcement under one bureau at the Commission ensures that staff, resources, and information are centralized and can be easily accessed by those who are the most impacted.

VI. Conclusion

Internet access is a requirement for contributing to our increasingly digital society. Higher connectivity rates means that consumers are generating an unprecedented amount of information without any idea of who has collected, stored, shared, and monetized critical pieces of their digital profiles. From shopping preferences, interests, and likes to more sensitive data such as online healthcare and banking information, consumers have a reasonable expectation of privacy and security when they are online.

The FTC has long been the arbiter of privacy policy in the United States and continues to be in the best position to bring together industry, academia, civil society, and public interest stakeholders to craft comprehensive data privacy rules. Ensuring that consumers are insulated from deceptive schemes and potential data mishandling is paramount in a healthy online ecosystem.