June 12th, 2024

Lina Khan, Chair Federal Trade Commission
Alvaro Bedoya, Commissioner
Andrew N. Ferguson, Commissioner
Melissa Holyoak, Commissioner
Rebecca Kelly Slaughter, Commissioner

Dear Chair Khan and Commissioners,

We write to urge the Federal Trade Commission (FTC) to put forth the Notice of Proposed Rulemaking on Commercial Surveillance and Data Security (NPRM).

Since the agency announced the Advanced Notice of Proposed Rulemaking (ANPRM) on commercial surveillance, the harmful impacts of unregulated surveillance and data collection have worsened. The volume, scope, and variety of sensitive information being collected and exploited has increased. It's become more common for corporations to surveil individuals that they don't have a commercial relationship with. Amazon's Ring surveillance devices **collect** biometric data from bystanders going about their daily lives. Meta **tracks** individuals as they browse the web regardless of whether they have an account, collecting and sharing detailed information with its Facebook platform.

The demand for new ways to surveil individuals and gather as much sensitive information as possible has reached an historic pitch. This demand is now primarily driven by Big Tech's race to dominate artificial intelligence (AI) and the need for large amounts of data to feed machine learning algorithms.

AI not only drives the increasing volume of data collected, it's also being leveraged by cybercriminals. Roughly 34% of the people residing in the United States have been **targets** of a cybercrime or hacking. From fraudulent charges on debit cards to hacked email accounts, lax data security practices, insecure data sharing between third-parties, and nonexistent data retention policies, vulnerabilities are compounding. These **attacks** are only increasing as AI facilitates rapid analysis and exploitation of such vulnerabilities and the data stolen through them. All of the information being gathered by the ubiquitous, mass commercial surveillance products and networks scattered throughout our communities, homes, stores, workplaces, and schools is more at risk than ever before.

Further, the rollback of constitutional privacy protections via the Supreme Court's decision in *Dobbs v. Jackson* has expanded the market demand for our day-to-day digital footprints. The decision ushered in a wave of state legislation allowing for prosecution of abortion seekers and providers. Such prosecutions can **rely** on data collected from the Wi-Fi enabled devices we use, the web based platforms we interact with, and the surveillance networks tracking our every move.

Right now, for a relatively low cost, anyone can pay a data broker to access an individual's home address, social security number, web browsing history, debit card transactions, and the locations they visit. In a 2022 **investigation**, Motherboard purchased the location data of visitors to 600 Planned Parenthood locations over the course of one week for $160. Although these laws are intended to target abortion seekers and providers, the precedents being set and the data collection models being developed to service them can be applied to anyone. In 2023, a **study** revealed how easy it is for anyone, including foreign governments, to purchase personal information about active duty members of the military-even allowing the purchaser to target military members based on which military base where they were stationed.

In discussing data exploitation and misuse, the disproportionate harms posed to Black, brown, Indigenous, and low income communities cannot be ignored or parceled out into another bucket of regulatory reforms. Black adults are more **likely** to be hacked than any other racial or ethnic group. Smartwatch trackers and phone applications are used to **track** and **monitor** migrants with no limits on the types of information that can be collected, the ways that information can be used, or the parties that information can be shared with. Companies, like ShotSpotter (recently renamed "SoundThinking"), sell products guised as technology that assists law enforcement and helps with neighborhood safety—when in actuality, their always-on microphones cannot accurately differentiate between a gunshot and other loud noises. These **devices** are disproportionately installed in mostly Black and brown communities across the country, and primarily serve as a way for ShotSpotter and other gun detection companies to surveil residents, collecting troves of data.

The FTC's mandate to protect against these harms is clear. While we were encouraged that the agency initiated the Rulemaking on Commercial Surveillance and Data Security, we're frustrated with the lack of action since the ANPRM.

It's incumbent upon the FTC to immediately move forward with the NPRM on Commercial Surveillance and Data Security. Additionally, the NPRM must address the harms and threats posed by surveillance and data-collecting companies. This includes, but is not limited to, prohibiting secondary data uses; bans on surveillance advertising and biometric data collection; restrictions on invasive, Wi-Fi enabled surveillance devices; ending the business model of sharing, trading, and selling individuals' personal data; and meaningful interventions to halt discrimination harms. The NPRM must also include protections for workers: addressing harmful worker surveillance; prohibiting automated surveillance that determines the pace of work; restricting automated decision-making without human oversight and an opportunity for workers to appeal; and banning the sharing and sale of workers' biometric and other sensitive data.

Ultimately, any rulemaking must ensure that people—regardless of race, immigration status, gender, sexual orientation, workplace, or income—retain total and not illusory control of their personal data and cannot be pressured by personal circumstance or lack of accessible alternatives to give that control away.

As core privacy rights are being challenged and data surveillance corporations are finding new ways to extract even more personal, sensitive data from individuals, we implore the FTC to put forth the NPRM on commercial surveillance. You must act now to protect the public at large, and do so regardless of any federal data privacy protections being discussed in Congress. We have waited long enough to prevent deceptive and unfair uses of data. Ultimately, both Congressional and agency interventions are needed to strengthen privacy protections into a blanket of interwoven laws and regulations that collectively protect individuals and their rights to privacy both now, and in the decades to come.

Sincerely,

Fight for the Future
Access Now
Advocacy For Principled Action In Government
Aspiration
Athena Coalition
Center on Race and Digital Justice
Constitutional Alliance
Consumer Federation of America
Demand Progress Education Fund
For the Many
Free Press
Generation Justice
Institute for Local Self-Reliance
Just Futures Law
Line Break Media
May First Movement Technology
Media Alliance
MediaJustice
Oakland Privacy
Open Markets Institute
Organization for Identity and Cultural Development (OICD.net)
PDX Privacy
Presente.org
Privacy Rights Clearinghouse
Project On Government Oversight
Restore The Fourth
RootsAction.org
Surveillance Technology Oversight Project
The Civil Liberties Defense Center
The Greenlining Institute
WA People's Privacy
Woodhull Freedom Foundation
Yale Privacy Lab