CHIME Cheat Sheet – September 9, 2022
The Federal Trade Commission (FTC) Advance Notice of Proposed Rulemaking (ANPR)
Commercial Surveillance and Data Security

Overview

On August 22, 2022, the Federal Trade Commission (FTC or Commission) published an Advance Notice of Proposed Rulemaking (ANPR) to request public comment on the prevalence of commercial surveillance and data security practices that harm consumers. In an "Advance Notice of Proposed Rulemaking" (ANPR), an agency evaluates possible alternative solutions to rulemaking and determines whether the benefits of the regulation justify the costs – before the traditional rulemaking process. Agencies typically submit an ANPR to the *Federal Register*, where the public has the opportunity to comment on the initial proposals and whether or not rulemaking should be initiated.

Specifically, the Commission is seeking comment on whether it should implement new trade regulation rules or other regulatory alternatives concerning the ways in which companies collect, aggregate, protect, use, analyze, and retain consumer data, as well as transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive. Additionally, the Commission released a Factsheet on Commercial Surveillance and Data Security and held a virtual public forum on September 8, 2022. Comments on the ANPR are due October 21, 2022.

Background & Summary

For more than two decades, the FTC has been the nation's privacy agency, engaging in policy work and bringing scores of enforcement actions concerning data privacy and security. These actions have alleged that certain practices violate Section 5 of the FTC Act or other statutes to the extent they pose risks to physical security, cause economic or reputational injury, or involve unwanted intrusions into consumers' daily lives. The Commission's extensive enforcement and policy work on these issues has raised important questions about the prevalence of harmful commercial surveillance and lax data security practices. This experience suggests that enforcement alone without rulemaking may be insufficient to protect consumers from significant harms.

The FTC is issuing this ANPR because recent Commission actions, news reporting, and public research suggest that harmful commercial surveillance and lax data security practices may be prevalent and increasingly unavoidable. Therefore, trade regulation rules reflecting the current realities may be needed to ensure Americans are protected from unfair or deceptive acts or practices. Additionally, new rules could also foster a greater sense of predictability for companies and consumers and minimize the uncertainty that case-by-case enforcement may engender.

The Commission is asking the public to weigh in on whether it should implement new trade regulation rules or other regulatory alternatives concerning the ways in which companies: 1) collect, aggregate, protect, use, analyze, and retain consumer data; as well as 2) transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive. The FTC is also seeking comment on: 1) the nature and prevalence of harmful commercial surveillance and lax data security practices; 2) the balance of costs and countervailing benefits of such practices for consumers and competition, as well as the costs and benefits of any given potential trade regulation rule; and 3) proposals for protecting consumers from harmful and prevalent commercial surveillance and lax data security practices.

The ANPR includes a wide range of issue areas the FTC is seeking comment on, with numerous questions related to each. The issue areas and topics include the following:

Commercial Surveillance & Consumer Harm Issue Areas
To What Extent Do Commercial Surveillance Practices or Lax Security Measures Harm Consumers?
To What Extent Do Commercial Surveillance Practices or Lax Data Security Measures Harm Children, including Teenagers?
How Should the Commission Balance Costs and Benefits?
How, if at All, Should the Commission Regulate Harmful Commercial Surveillance or Data Security Practices that Are Prevalent?
Data Security
Collection, Use, Retention, and Transfer of Consumer Data
Automated Decision-making Systems
Discrimination Based on Protected Categories
Consumer Consent
Notice, Transparency, and Disclosure
What Are the Mechanisms for Opacity?
Who Should Administer Notice or Disclosure Requirements?
What Should Companies Provide Notice of or Disclose?
Remedies
Obsolescence

Consumer Surveillance

Commercial surveillance is the business of collecting, analyzing, and profiting from information about people. Technologies essential to everyday life also enable near constant surveillance of people's private lives. The volume of data collected exposes people to identity thieves and hackers. Mass surveillance has heightened the risks and stakes of errors, deception, manipulation, and other abuses. FTC enforcement actions, news reports, and published research indicate that the commercial surveillance industry is increasingly unavoidable. Further, these developments suggest that new rules reflecting these current realities may be needed to ensure Americans are protected from unfair or deceptive acts or practices. The FTC notes that these rules could also foster a greater sense of predictability for companies and consumers – and minimize the uncertainty that case-by-case enforcement can lead to. In this ANPR, the following terms are defined as:

- **Data security** – refers to breach risk mitigation, data management and retention, data minimization, and breach notification and disclosure practices.
- **Commercial surveillance** – refers to the collection, aggregation, analysis, retention, transfer, or monetization of consumer data and the direct derivatives of that information. These data include both information that consumers actively provide—say, when they affirmatively register for a service or make a purchase—as well as personal identifiers and other information that companies collect, for example, when a consumer casually browses the web or opens an app. This latter category is far broader than the first.
- **Consumer** – includes businesses and workers, not just individuals who buy or exchange data for retail goods and services. This approach is consistent with the Commission's longstanding practice of bringing enforcement actions against firms that harm companies as well as workers of all kinds. The FTC has frequently used Section 5 of the FTC Act to protect small businesses or individuals in contexts involving their employment or independent contractor status.

According to the FTC, most Americans – whether they know it or not – surrender their personal information to engage in the most basic aspects of modern life. The Commission notes that when consumers, for example, buy groceries, do homework, and apply for car insurance, they are likely giving a wide range of personal information about themselves to companies. This information can include their movements, prayers, friends, menstrual cycles, web-browsing, and faces, among other basic and intimate aspects of their lives.

Companies continue to develop and market products and services to collect and monetize this data. The FTC notes that an "elaborate and lucrative market for the collection retention, aggregation, analysis, and onward disclosure of consumer data incentivizes many of the services and products on which people have come to rely." Businesses claim to use personal information to target services – specifically, to set prices, curate newsfeeds, serve advertisements, and conduct research on people's behavior, among other things." The Commission notes that while, in theory, these personalization practices have the potential to benefit consumers, reports indicate that they have facilitated consumer harms that can be difficult if not impossible for any individual to avoid.

The FTC is concerned that companies have strong incentives to develop products and services that track and surveil consumers' online activities as much as possible. Further, these companies refine their proprietary automated systems to better predict consumer behavior. Key features of the commercial surveillance industry include collection; analysis; and monetization. The Commission is seeking comment on a wide array of concerns stemming from the collection, analysis and monetization in commercial surveillance – including lax data security; harms to children; retaliation; surveillance creep; inaccuracy; bias and discrimination; and dark patterns.

- **Collection:** The FTC is concerned that companies are collecting "vast troves of consumer information", while consumers are proactively sharing only a small fraction of this data. The Commission asserts that much of this data is "collected through secret surveillance practices" – noting that companies can track every aspect of consumers' engagement online. Further, companies can surveil them while they are connected to the internet – including their family and friend networks, browsing and purchase histories, location and physical movements, and a wide range of other personal details. Data can be collected by companies in many other ways, such as purchasing it from data brokers and pulling it from public sources.
- **Analysis:** The FTC is concerned that companies use algorithms and automated systems to analyze the information they collect. They can then build consumer profiles and make inferences about them to predict their behavior and preferences – and "may analyze this information without regard for the context in which it was collected."
- **Monetization:** The FTC is concerned that companies monetize surveillance in a wide variety of ways. Companies may use some of the information they collect to provide products and services, but they can also use it to make money. For example, they may sell the information through the massive, opaque market for consumer data, use it to place behavioral ads, or leverage it to sell more products.

Furthermore, some companies reportedly claim to collect consumer data for one stated purpose, but also use it for other purposes. For example, they sell or otherwise monetize such information or compilations of it in their dealings with advertisers, data brokers, and other third parties. Companies engage in these practices pursuant to the ostensible consent they obtain from consumers – however, as networked devices and online services become essential to navigating daily life, consumers may have little choice but to accept the terms that are offered. The FTC notes that reports suggest that consumers have become resigned to the ways in which companies collect and monetize their information – largely because they have little to no actual control over what happens to their information once companies collect it.

Privacy notices that acknowledge these risks are largely unreadable to the average consumer; furthermore, many do not have the time to review lengthy privacy notices for each of their devices, applications, websites, or services – let alone the periodic updates to them. The Commission believes that if consumers do not have meaningful access to this information, they cannot make informed decisions about the costs and benefits of using different services. Furthermore – the FTC believes the "information asymmetry" between companies and consumers runs even deeper. The companies collecting and using the information they collect are used in ways that are not often apparent, and in ways that go well beyond merely providing the products or services consumers believed that they signed up for.

To date, the Commission's enforcement actions have targeted "several pernicious dark pattern practices" – including burying privacy settings behind multiple layers of the user interface and making misleading representations to ''trick or trap'' consumers into providing personal information. In other cases, firms may misrepresent or fail to communicate clearly how they use and protect people's data. The FTC states that

given the reported scale and pervasiveness of such practices, individual consumer consent may be irrelevant.

Harms to Consumers

This ANPR has alluded to only a fraction of the potential consumer harms arising from lax data security or commercial surveillance practices, including those concerning physical security, economic injury, psychological harm, reputational injury, and unwanted intrusion.

The permissions that consumers give may not always be meaningful or informed. The FTC notes studies have shown that most people do not generally understand the market for consumer data. A majority of consumers know little about the data brokers and third parties who collect and trade consumer data or build consumer profiles – which can expose intimate details about their lives, and in the wrong hands, could expose them to future harm.

Material harms of commercial surveillance practices can be substantial – furthermore, they may be exacerbated due to the increase in risks of cyberattack by hackers, data thieves, and other bad actors. Lax data security practices could impose "enormous financial and human costs." Furthermore, fraud and identity theft cost both businesses and consumers billions of dollars – and consumer complaints have increased.

Finally, companies' growing reliance on automated systems is creating new forms and mechanisms for discrimination based on statutorily protected categories, including in critical areas such as housing, employment, and healthcare. The FTC notes several recent examples and reports including how some employers' automated systems have reportedly learned to promote and prefer men over women. A recent investigation suggested that lenders' use of educational attainment in credit underwriting might disadvantage students who attended historically Black colleges and universities (HBCUs). And the Department of Justice (DOJ) recently settled its first case challenging algorithmic discrimination under the Fair Housing Act for a social media advertising delivery system that unlawfully discriminated based on protected categories. Critically, these kinds of disparate outcomes may arise even when automated systems consider only unprotected consumer traits.

FTC Rulemaking Process

Issuing the Commercial Surveillance and Data Security ANPR is the beginning of the FTC rulemaking process. It invites the public to provide input on: (a) the nature and prevalence of harmful commercial surveillance practices; (b) the balance of costs and countervailing benefits of such practices for consumers and competition; and (c) proposals for protecting consumers from harmful and prevalent commercial surveillance practices.

Through this ANPR, the Commission aims to generate a public record about prevalent commercial surveillance practices or lax data security practices that are unfair or deceptive, as well as efficient, effective, and adaptive regulatory responses. These comments will help to sharpen the Commission's enforcement work and may inform reform by Congress or other policymakers, even if the Commission does not ultimately promulgate new trade regulation rules. The FTC indicates that they expect this ANPR to generate significant interest. Additionally, his ANPR does not identify the full scope of potential approaches the Commission might ultimately undertake by rule or otherwise. It does not delineate a boundary on the issues on which the public may submit comments. Further, it does not constrain the actions the Commission might pursue in an NPRM or final rule.

Key Links & Resources

- FTC Press Release
- ANPR regarding Commercial Surveillance and Data Security
- Fact Sheet on Commercial Surveillance and Data Security
- Fact Sheet on Public Participation in the Section 18 Rulemaking Process
- Virtual Public Forum Agenda – September 8, 2022