Commercial Surveillance and Data Security Rulemaking

Tags: Consumer Protection

Date: August 11, 2022

Factsheet on Commercial Surveillance and Data Security (213.57 KB)

Advance Notice of Proposed Rulemaking regarding Commercial Surveillance and Dat...

Factsheet on Public Participation in the Section 18 Rulemaking Process

Participación Pública En El Proceso De Reglamentación De La FTC Conforme a La S...

Overview

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. The Federal Trade Commission is asking the public to weigh in on whether new rules are needed to protect people's privacy and information in the commercial surveillance economy.

Public Forum

The Commission is hosting a public forum on commercial surveillance and data security to be held virtually on Thursday, September 8, 2022, from 2 p.m. until 7:30 p.m. Members of the public are invited to attend. Learn more on the Commercial Surveillance and Data Security Public Forum page.

Submit a Comment

The Advanced Notice of Proposed Rulemaking asks a series of questions about practices related to commercial surveillance and data security. The topic areas and the questions are listed below. Anyone from the public can submit a comment weighing in on the rulemaking, the general topics, or a specific question.

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.

- Which practices do companies use to surveil consumers?
- Which measures do companies use to protect consumer data?
- Which of these measures or practices are prevalent? Are some practices more prevalent in some sectors than in others?
- How, if at all, do these commercial surveillance practices harm consumers or increase the risk of harm to consumers?
- Are there some harms that consumers may not easily discern or identify? Which are they?
- Are there some harms that consumers may not easily quantify or measure? Which are they?
- How should the Commission identify and evaluate these commercial surveillance harms or potential harms? On which evidence or measures should the Commission rely to substantiate its claims of harm or risk of harm?
- Which areas or kinds of harm, if any, has the Commission failed to address through its enforcement actions?
- Has the Commission adequately addressed indirect pecuniary harms, including potential physical harms, psychological harms, reputational injuries, and unwanted intrusions?
- Which kinds of data should be subject to a potential trade regulation rule? Should it be limited to, for example, personally identifiable data, sensitive data, data about

protected categories and their proxies, data that is linkable to a device, or non-aggregated data? Or should a potential rule be agnostic about kinds of data?

- Which, if any, commercial incentives and business models lead to lax data security measures or harmful commercial surveillance practices? Are some commercial incentives and business models more likely to protect consumers than others? On which checks, if any, do companies rely to ensure that they do not cause harm to consumers?

- Lax data security measures and harmful commercial surveillance injure different kinds of consumers (e.g., young people, workers, franchisees, small businesses, women, victims of stalking or domestic violence, racial minorities, the elderly) in different sectors (e.g., health, finance, employment) or in different segments or "stacks" of the internet economy. For example, harms arising from data security breaches in finance or healthcare may be different from those concerning discriminatory advertising on social media which may be different from those involving education technology. How, if at all, should potential new trade regulation rules address harms to different consumers across different sectors? Which commercial surveillance practices, if any, are unlawful such that new trade regulation rules should set out clear limitations or prohibitions on them? To what extent, if any, is a comprehensive regulatory approach better than a sectoral one for any given harm?

Harms to Children

Costs and Benefits

Regulations

Automated Systems

Discrimination

Consumer Consent

Notice, Transparency, and Disclosure

Remedies

Obsolescence