FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Technology Blog

Cars & Consumer Data: On Unlawful Collection & Use

By: Staff in the Office of Technology and The Division of Privacy and Identity Protection | May 14, 2024

Some say the car a person drives can say a lot about them. As cars get "connected," this turns out to be truer than many people might have realized. While connectivity can let drivers do things like play their favorite internet radio stations or unlock their car with an app, connected cars can also collect a lot of data about people. This data could be sensitive—such as biometric information or location—and its collection, use, and disclosure can threaten consumers' privacy and financial welfare.

Connected cars have been on the FTC's radar for years. The FTC highlighted concerns related to connected cars as part of an "Internet of Things" workshop held in 2013, followed by a 2015 report. In 2018, the FTC hosted a connected cars workshop highlighting issues ranging from unexpected secondary uses of data to security risks. The agency has also published guidance to consumers reminding them to wipe the data on their cars before selling them—much as anyone would when trying to resell a computer or smart phone.

Over the years, privacy advocates have raised concerns about the vast amount of data that could be collected from cars, such as biometric, telematic, geolocation, video, and other personal information. News reports have also suggested that data from connected cars could be used to stalk people or affect their insurance rates. Many have noted that when any company collects a large amount of sensitive data, it can pose national security issues if that data is shared with foreign actors.

Car manufacturers—and all businesses—should take note that the FTC will take action to protect consumers against the illegal collection, use, and disclosure of their personal data. Recent enforcement actions illustrate this point:

- **Geolocation data is sensitive and subject to enhanced protections under the FTC Act.** Cars are much like mobile phones when it comes to revealing consumers' persistent, precise location. In a series of seminal cases in recent years, the Commission has established that the collection, use, and disclosure of location can be an unfair practice. In X-Mode, the FTC alleged that the data could be used to track people's visits to sensitive locations like medical or reproductive health clinics, places of worship, or domestic abuse shelters. Similarly, in InMarket, the Commission alleged that the company's internal use of sensitive data to group consumers into highly sensitive categories for advertising purposes was unlawful. The orders resolving these matters prohibit these companies from selling sensitive location information.

- **Surreptitious disclosure of sensitive information can be an unfair practice.** Companies that have legitimate access to consumers' sensitive information must ensure that the data is used only for the reasons they collected that information. For example, the Commission recently alleged that BetterHelp, which offers online counseling services—including those marketed to specific groups like Christians, teens, and the LGBTQ+ community—revealed consumers' email addresses and health questionnaire information to third parties for advertising purposes. Similarly, the Commission took action against mental telehealth provider Cerebral for, among other things, the company's unfair privacy and security practices. The FTC obtained settlements requiring BetterHelp and Cerebral to pay millions of dollars so that affected consumers could receive partial refunds, and the Cerebral settlement bans the company from using or disclosing consumers' personal information for advertising purposes.

- **Using sensitive data for automated decisions can also be unlawful.** Companies that feed consumer data into algorithms may be liable for harmful automated decisions. The FTC recently took action against Rite Aid, saying in a complaint that the company enrolled people into a facial recognition program that alerted employees when suspected matches entered their stores. The complaint includes allegations that Rite Aid failed to take reasonable steps to prevent low-quality images from being used with the program, increasing the likelihood of false-positive match alerts. In some cases, false alerts came with recommended actions, such as removing people from the store or calling the police, and employees followed through on those recommendations. As a result of the FTC's action, Rite Aid agreed to a 5-year ban on the use of facial recognition technology.

These cases underscore the significant potential liability associated with the collection, use, and disclosure of sensitive data, such as biometrics and location data. As the FTC has stated, firms do not have the free license to monetize people's information beyond purposes needed to provide their

requested product or service, and firms shouldn't let business model incentives outweigh the need for meaningful privacy safeguards.

The easiest way that companies can avoid harming consumers from the collection, use, and sharing of sensitive information is by simply not collecting it in the first place. When they are motivated to, all businesses—including auto manufacturers—are capable of building products with safeguards that protect consumers.

Thank you to staff from across the Office of Technology and the Division of Privacy and Identity Protection in the Bureau of Consumer Protection who collaborated on this post.

Tags: Consumer Protection | Privacy and Security | Consumer Privacy | Data Security | Office of Technology

More from the Technology Blog

Technology Blog

The FTC Is on the Front Lines of Tech Innovation & Regulation

Stephanie T. Nguyen, Chief Technologist | January 17, 2025

Technology Blog

Behind the FTC's 6(b) Report on Large AI Partnerships & Investments

Office of Technology Staff | January 17, 2025

Technology Blog

Surveillance Pricing Update & The Work Ahead

Stephanie T. Nguyen & Samuel A.A. Levine | January 17, 2025

Technology Blog

Lenses of security: Preventing and mitigating digital security risks through data management, software development, and product design for humans

Staff in the Office of Technology & the Division of Privacy and Identity Protection | December 13, 2024

Get Business Blog updates

Enter email address

Subscribe