Business Blog

Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data

By: Kristin Cohen, Acting Associate Director, FTC Division of Privacy & Identity Protection July 11, 2022

Among the most sensitive categories of data collected by connected devices are a person's precise location and information about their health. Smartphones, connected cars, wearable fitness trackers, "smart home" products, and even the browser you're reading this on are capable of directly observing or deriving sensitive information about users. Standing alone, these data points may pose an incalculable risk to personal privacy. Now consider the unprecedented intrusion when these connected devices and technology companies collect that data, combine it, and sell or monetize it. This isn't the stuff of dystopian fiction. It's a question consumers are asking right now.

The conversation about technology tends to focus on benefits. But there is a behind-the-scenes irony that needs to be examined in the open: the extent to which highly personal information that people choose not to disclose even to family, friends, or colleagues is actually shared with complete strangers. These strangers participate in the often shadowy ad tech and data broker ecosystem where companies have a profit motive to share data at an unprecedented scale and granularity.

When consumers use their connected devices – and sometimes even when they don't – these devices may be regularly pinging cell towers, interacting with WiFi networks, capturing GPS signals, and otherwise creating a comprehensive record of their whereabouts. This location data can reveal a lot about people, including where we work, sleep, socialize, worship, and seek medical treatment. While many consumers may happily offer their location data in exchange for real-time crowd-sourced

advice on the fastest route home, they likely think differently about having their thinly-disguised online identity associated with the frequency of their visits to a therapist or cancer doctor.

Beyond location information generated automatically by consumers' connected devices, millions of people also actively generate their own sensitive data, including by using apps to test their blood sugar, record their sleep patterns, monitor their blood pressure, or track their fitness, or sharing face and other biometric information to use app or device features. The potent combination of location data and user-generated health data creates a new frontier of potential harms to consumers.

The marketplace for this information is opaque and once a company has collected it, consumers often have no idea who has it or what's being done with it. After it's collected from a consumer, data enters a vast and intricate sales floor frequented by numerous buyers, sellers, and sharers. There are the mobile operating systems that provide the mechanisms for collecting the data. Then there are app publishers and software development kit (SDK) developers that embed tools in mobile apps to collect location information and provide the data to third parties.

The next stop in the murky marketplace may be data aggregators and brokers – companies that collect information from multiple sources and then sell access to it (or analyses derived from it) to marketers, researchers, and even government agencies. These companies often build profiles about consumers and draw inferences about them based on the places they have visited. The amount of information they collect is staggering. For example, in a 2014 study, the FTC reported that data brokers use data to make sensitive inferences, such as categorizing a consumer as "Expectant Parent." According to the report, one data broker bragged to shareholders in a 2013 annual report that it had 3,000 points of data for nearly every consumer in the United States. In many instances, data aggregators and brokers have no interaction with consumers or the apps they're using. So people are left in the dark about how companies are profiting from their personal information.

Now let's consider a particularly sensitive subset at the intersection of location and health: information related to personal reproductive matters – for example, products that track women's periods, monitor their fertility, oversee their contraceptive use, or even target women considering abortion.

The concerns many have expressed about the risk of misuse are more than just theoretical. In 2017, for example, the Massachusetts Attorney General reached a settlement with marketing company Copley Advertising, LLC, and its principal for using location technology to identify when people crossed a secret digital "fence" near a clinic offering abortion services. Based on that data, the

company sent targeted ads to their phones with links to websites with information about alternatives to abortion. The Massachusetts AG asserted that the practice violated state consumer protection law.

And just recently, the FTC reached a settlement with Flo Health, alleging the company shared with third parties – including Google and Facebook – sensitive health information about women collected from its period and fertility-tracking app, despite promising to keep this information private.

The misuse of mobile location and health information – including reproductive health data – exposes consumers to significant harm. Criminals can use location or health data to facilitate phishing scams or commit identity theft. Stalkers and other criminals can use location or health data to inflict physical and emotional injury. The exposure of health information and medical conditions, especially data related to sexual activity or reproductive health, may subject people to discrimination, stigma, mental anguish, or other serious harms. Those are just a few of the potential injuries – harms that are exacerbated by the exploitation of information gleaned through commercial surveillance.

The Commission is committed to using the full scope of its legal authorities to protect consumers' privacy. We will vigorously enforce the law if we uncover illegal conduct that exploits Americans' location, health, or other sensitive data. The FTC's past enforcement actions provide a roadmap for firms seeking to comply with the law.

What should companies consider when thinking about the collection of confidential consumer information, including location and health data?

Sensitive data is protected by numerous federal and state laws. There are numerous state and federal laws that govern the collection, use, and sharing of sensitive consumer data, including many enforced by the Commission. The FTC has brought hundreds of cases to protect the security and privacy of consumers' personal information, some of which have included substantial civil penalties. In addition to Section 5 of the FTC Act, which broadly prohibits unfair and deceptive trade practices, the Commission also enforces the Safeguards Rule, the Health Breach Notification Rule, and the Children's Online Privacy Protection Rule.

Claims that data is "anonymous" or "has been anonymized" are often deceptive. Companies may try to placate consumers' privacy concerns by claiming they anonymize or aggregate data. Firms making claims about anonymization should be on guard that these claims can be a deceptive trade practice and violate the FTC Act when untrue. Significant research has shown that "anonymized" data can often be re-identified, especially in the context of location data. One set of researchers demonstrated that, in some instances, it was possible to uniquely identify 95% of a dataset of 1.5 million individuals

using four location points with timestamps. Companies that make false claims about anonymization can expect to hear from the FTC.

The FTC cracks down on companies that misuse consumers' data. As recent cases have shown, the FTC does not tolerate companies that over-collect, indefinitely retain, or misuse consumer data. Ad exchange OpenX recently paid $2 million for collecting children's location data without parental consent. The Commission also took action against Kurbo/Weight Watchers for, among other things, indefinitely retaining sensitive consumer data. The settlement requires the company to pay a $1.5 million fine for violating COPPA, delete all illegally collected data, and also delete any work product algorithms created using that data. Just a few weeks ago, the Commission entered a final order requiring CafePress to pay redress and minimize its data collection because, according to the Commission's complaint, it improperly collected and retained consumer data, and failed to respect consumers' deletion requests, among other things.

The FTC has additional guidance for businesses on consumer privacy and data security. Also, read the latest from the Department of Health & Human Services on the topic.

Tags: Consumer Protection | Bureau of Consumer Protection | Privacy | Privacy and Security | Consumer Privacy | Tech | Health Privacy

Comments closed.

Toni LaPoint July 27, 2022

As one that tried Louisiana. Gov website for pandemic help, I am now bombarded with unknown phone calls/ text messages and emails constantly. Being offered rediculous things. Just give account information to receive. It horrifies me that much ur governor is still allowing this to continue on a government site where most older adults like myself feel safe. SOO very grateful the FTC is looking in to this.

Elizabeth Tulles July 27, 2022

I have been warning about this for years. While I applaud your efforts, I doubt you will be able to make much headway against the data brokers and corporate interests that make so much money from buying

and selling personal information that is not theirs.

There is a reason we are the only country in the world without without a strong federal privacy law.

Jill Edwards August 29, 2022

Perhaps if consumers were notified when their data is being sold BY and TO who and given a chance to SIMPLY opt out of their data being sold and further collected by the seller, we would feel safer and more aware of the who, what, when, where and how our devices are divulging such private and personal data and be given an opportunity to EASILY protect ourselves. Many of us older consumers are technologically challenged and don't understand the terminology used in the settings that were automatically activated upon phone set up or app installation.

L de Bivort August 29, 2022

Isn't it way past due to enact a STRONG personal privacy law? The Europeans have done it; don't we Americans deserve (and need) it too?

More from the Business Blog

Business Blog

No shortcuts to five stars: Lessons from the FTC's settlement with Sitejabber

Julia Solomon Ensor | November 6, 2024

Business Blog

The FTC frowns on franchise falsehoods: A reminder to franchisors

Julia Solomon Ensor | October 16, 2024

Business Blog

Click to Cancel: The FTC's amended Negative Option Rule and what it means for your business

Julia Solomon Ensor | October 16, 2024

Business Blog

Mark your calendars, telemarketers and sellers! October 15 is the Telemarketing Sales Rule's Record Store Day.

Ben Davidson | October 11, 2024