BRENNAN CENTER FOR JUSTICE

Congress Must Close the Data Broker Loophole by Prohibiting Government Purchases of Americans' Sensitive Data

The Problem

Privacy laws in this country are badly outdated, creating gaps that data brokers and government agencies can exploit. For instance, the Electronic Communications Privacy Act prohibits phone and internet companies from selling sensitive customer data to government agencies. But the law doesn't address digital data brokers because they barely existed in 1986, when the law was passed. Companies that are barred from selling data to the government can thus sell to data brokers instead, and the brokers can sell the same data to the government—for a handsome profit. The data is effectively laundered through a middleman.

The government is even buying its way around the Fourth Amendment. In 2018, the Supreme Court held that the government needs a warrant to obtain cell phone location records because they can reveal highly sensitive information about our private lives. But government lawyers interpret this ruling to apply only when the government *compels* disclosure of the records—not when it merely *incentives* disclosure by writing a big check. Federal agencies are thus buying up massive databases of Americans' cell phone location information without any legal process whatsoever.

AI supercharges risks to privacy and civil liberties. AI tools allow government agencies to collect and analyze information on a previously unimaginable scale to create a comprehensive picture of Americans' private lives. The Department of Defense is reportedly demanding that it be able to use AI to collect and analyze Americans' information, including web-browsing and location records.

Federal agencies are routinely exploiting this loophole:

- The FBI, the Drug Enforcement Administration, the Department of Homeland Security (including CBP, ICE, and the Secret Service), the Department of Defense, and even the Internal Revenue Service have reportedly bought access to Fourth Amendment-protected location data.
- CBP has tapped into the online advertising industry to purchase Americans' personal data, and ICE recently bought access to hundreds of millions of people's mobile location records. A DHS Inspector General report revealed that CBP, ICE, and the Secret Service purchased cell phone location data without complying with DHS privacy policies or performing statutorily required Privacy Impact Assessments.
- The Department of Defense purchased "granular location data" harvested from a popular Muslim prayer app used by 98 million people around the world, including Americans, as well as similar data generated by a Muslim dating app.
- The NSA purchases information about Americans' internet activity from data brokers—including communications metadata for wholly domestic communications, which can reveal a person's associations, habits, and even beliefs.
- Data brokers collect and sell information about activities protected by the U.S. and/or state constitutions. For instance, brokers have sold location information of people visiting abortion providers and could easily do the same for people visiting gun stores.

BRENNAN CENTER FOR JUSTICE

- A working group commissioned by the Office of the Director of National Intelligence issued the ominous warning that no one in the intelligence community knows precisely what information has been purchased or how it is used.

The Solution

The bipartisan Fourth Amendment Is Not For Sale Act would prohibit law enforcement and intelligence agencies from purchasing certain sensitive information from third-party sellers, including geolocation information, communications-related information that is protected under the Electronic Communications Privacy Act, and information obtained through illegitimate scraping practices. Likewise, provisions in the bipartisan Government Surveillance Reform Act and the Security and Freedom Enhancement Act would prohibit law enforcement and intelligence agencies from purchasing a wide range of sensitive information. Under all of these bills, agencies would still be able to obtain the information using a warrant, court order, or subpoena, as provided by law.

This solution has overwhelming popular support. **Polling shows that 80% of Americans support requiring the government to obtain a warrant before purchasing location information, internet records, and other sensitive data about Americans.**

What Opponents Will Say — and Why They're Wrong

- **"If private entities can buy this data, the government should also be able to buy it."** Congress can and should consider comprehensive consumer data privacy legislation to address the private market in our data. But in the meantime, government purchases of sensitive data pose a unique threat to civil liberties. The government has coercive powers over the people of this country that private entities don't have: it can arrest, imprison, deport, tax, audit, fine, deny public benefits, and take a host of other actions directly impacting our freedoms. And of course, the government alone is bound by the Fourth Amendment—a constraint it is evading through data purchases.
- **"The U.S. government will be at a disadvantage because hostile foreign governments like China can still buy this data."** The Department of Justice has implemented rules limiting the export of sensitive data to certain foreign nations, including China, Cuba, Iran, North Korea, Russia, and Venezuela. In any case, the fact that China does not respect the privacy rights of U.S. citizens is no justification for the U.S. government to show the same disrespect. The Fourth Amendment holds our government to a higher standard, and rightly so. Adopting the rationale that "if the Chinese government can do it, the U.S. government should be able to do it" would launch a race to the bottom with grave implications for Americans' freedoms across a range of government practices.
- **"These bills would risk public safety by putting restrictions on law enforcement access to data."** The government's practice of purchasing bulk cell phone location information and other protected sensitive data from data brokers is a relatively new phenomenon. Until quite recently, law enforcement officers were required to obtain warrants, court orders, and subpoenas to obtain the information covered by this bill. Opponents of these bills have put forward no evidence that complying with these longstanding legal privacy protections was harmful to public safety. These bills simply close the loophole that has allowed law enforcement to circumvent these protections.

For questions about how to close the data broker loophole, contact Liza Goitein at goiteine@brennan.law.nyu.edu or Emile Ayoub at ayoube@brennan.law.nyu.edu.