BRENNAN
CENTER
FOR JUSTICE

Congress Must Close 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Privacy laws in this country are badly outdated, creating gaps that data brokers and government agencies can exploit.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, let alone a warrant.

The facts are sobering:

- The list of federal agencies that reportedly have bought access to Fourth Amendment-protected data includes the FBI, the Drug Enforcement Administration, multiple components of the Department of Homeland Security (including Customs and Border Protection, Immigration and Customs Enforcement, and the Secret Service), and the Department of Defense. Even the Internal Revenue Service "attempted to identify and track potential criminal suspects by purchasing access to a commercial database that records the locations of millions of American cellphones."
- 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.
- 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 has confirmed that it purchases information about Americans' internet activity from data brokers. This includes "netflow data," i.e., communications metadata, including for wholly domestic communications. Communications metadata can reveal a person's associations, habits, and even beliefs.
- A DHS Inspector General report revealed that CBP, ICE, and the Secret Service purchased communications information without complying with DHS privacy policies or performing statutorily required Privacy Impact Assessments.
- 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 Fourth Amendment Is Not For Sale Act (or similar legislation) should be incorporated into legislation reauthorizing Section 702. This bill 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. The bill contains exceptions for emergencies, and law enforcement and intelligence agencies would still be able to obtain the information using a warrant, court order, or subpoena, as provided by law.

This solution has broad bipartisan and popular support. The Fourth Amendment Is Not For Sale Act was reported out of the House Judiciary Committee by a unanimous vote (with just one member voting "present"). **Recent 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

- **"This has nothing to do with Section 702."** Section 702 is one piece of a vast network of often-overlapping surveillance authorities. If one avenue of warrantless surveillance is closed off, the government will often be able to switch to another authority—or exploit gaps in the law, like the data broker loophole, that permit surveillance with no statutory authorization at all. Reforming Section 702 in isolation without addressing the data broker loophole is the equivalent of sealing off one of two giant breaches in a dam.

- **"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."** President Biden will soon issue an executive order directing his administration to promulgate regulations limiting the export of sensitive data to certain foreign nations. Lawmakers have also introduced legislation to do the same. In the meantime, 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.

For questions about ending the warrantless surveillance of Americans, contact Liza Goitein at goiteine@brennan.law.nyu.edu or Noah Chauvin at chauvinn@brennan.law.nyu.edu.