Wyden Remarks on Secret Law and the Fourth Amendment is Not for Sale Act for the Cato Institute

December 14, 2021

Thank you for having me here at the Cato Institute. Julian and the rest of this institution are proof that defending Americans' civil liberties is not a partisan proposition.

Today, I'm going to talk about how the government is using its credit card to erase Americans' Constitutional rights. And how Rand Paul, Steve Daines, Mike Lee, Majority Leader Schumer, Chairman Leahy, a host of other Democrats and I have a bipartisan bill to end this outrageous end-run around the Fourth Amendment.

One of the most important issues with surveillance and privacy is being fought on a new front, one that many Americans, including most of Congress, know virtually nothing about - multiple federal agencies, including the Internal Revenue Service, the Department of Defense and Department of Homeland Security, have purchased Americans' data without any court oversight whatsoever.

This problem goes back to the Electronic Communication Privacy Act in the 1980s. That law only protects data held by companies with whom consumers have a direct relationship. Companies like Google, Facebook, Apple, and telephone companies like AT&T and Verizon are all covered. These companies can only share our data with the government under a strict set of circumstances, most of which require a court order.

This includes metadata. While ECPA [pronounced: eck-pah] doesn't require a warrant for the government to demand our metadata, it does require a court order - one that is easier to get, but that still has to be authorized by an independent judge - for disclosures of most metadata.

While Congress in 1986 strictly regulated government surveillance involving tech and telecom companies - at least those that provide services to the public - it did not prevent them from sharing our metadata with other third parties. ECPA contained loopholes that allowed tech and telecom companies to share, and sell, to other companies, metadata about the web pages we read, the apps we download, and the places we go.

Once a tech or telecom company sells our information to someone else, like a data broker, that information has no protections under either ECPA or the third-party doctrine. Right now shady middlemen can sell our personal information to the government without any kind of court order.

In another loophole, technology infrastructure companies are also not covered by ECPA. When someone using Gmail sends an email to a user of Yahoo mail, that email will likely pass through several companies that own or operate fiber optic cables, cell towers, and internet exchanges. These infrastructure companies are ALSO not covered by federal privacy law, and so they can share or sell our metadata to the government.

This is an issue I've been concerned about for more than ten years. As a member of the Senate Intelligence Committee, I have access to classified information about the intelligence community and other parts of our government. I'm able to see their

secret interpretations of the law, in order to legislate and conduct oversight, but I'm often not able to reveal the details of what I've learned.

Some of you will remember about my fight with the National Security Agency, over their Orwellian interpretation of Section 215, part of the Foreign Intelligence Surveillance Act, which they used for years to obtain, in bulk, phone records about millions of Americans' communications. The government had adopted a twisted reading of this law, and gotten the nation's top secret surveillance court, to sign off on it, while the public was kept in the dark. I'm a firm believer that while it may be necessary to keep secret the sources and methods of surveillance - the law, and how the government has interpreted it, should never be kept secret from the American people.

On this particular problem - companies selling Americans' data to the government - I've been pushing on two fronts.

I've been leading an investigation into the sale of Americans' location data since 2018. My first target was the major phone companies - AT&T, Verizon, T-Mobile, and Sprint - who I caught selling data to shady data brokers that let prison guards and local law-enforcement agencies track any phone in America without any kind of court order. Investigative journalists soon discovered the same data brokers were also selling location data to bounty hunters, used car salesmen, and would-be stalkers.

Based on my work, and the diligent work of journalists, the Federal Communications Commission fined the carriers $200 million dollars. While this is a win for consumers and their privacy, the wireless carriers are fighting the fines,

and are arguing that they have the legal right to sell huge amounts of their customers' data.

Beyond wireless carriers, there are plenty of other corporations selling location data collected from Americans' phones. The advertising technology industry has more than picked up the slack. How does this work?

When you install a smartphone app - let's say a weather app - and it asks you for permission to access your location data - 3rd party data broker companies are able to piggyback on that permission and collect information from your phones, which they sell onwards. These data brokers typically pay app developers a fee for the data they are siphoning off.

In February of 2021, the Wall Street Journal reported that Venntel, a shady data broker in Virginia, was buying location data generated from smartphone apps, packaging it up for access through an easy-to-use website, and selling access to government agencies for thousands of dollars a pop. Venntel has sold data to CBP, ICE, the DEA, and IRS.

So far, I've confirmed that two agencies - the IRS and CBP have used this tool, without any kind of court supervision, to track Americans' phones. And just last week I succeeded in pushing utility companies to end their practice of letting data brokers sell their customers' private information to law-enforcement agencies and private investigators.

These practices amount to an outrageous privacy violation and a shameless end run around the 4th Amendment. These agencies would need a court order to obtain

location data from AT&T and Verizon, or from Google and Facebook, but they're exploiting the data broker loophole. Venntel isn't the only company - there are several data brokers involved in this industry, and they are the target of my ongoing oversight investigation.

It's still not clear why these agencies have been able to buy location data, from any source, after the Supreme Court's *Carpenter* decision. The court did not create a special exception in the 4th Amendment for data brokers or allow the government to bypass the courts as long as they paid for information. I've asked several government agencies for copies of the legal opinions they relied on to use this data without a court order, and I'm not giving up until I get some answers.

These companies need to be shut down and Congress needs to step in to prevent the government from using a credit card instead of a warrant.

Friends shouldn't filibuster friends, so I'll wrap things up with two points about how we can end these shady practices.

First, I've introduced a bipartisan bill with Senators Paul, Daines, and Lee called the Fourth Amendment is Not for Sale Act, which has broad support from everyone from Senator Schumer to FreedomWorks.

It would essentially ban the government from buying or otherwise obtaining information from a data broker that would otherwise require a court order. In my view, it's essential to prevent data brokers from acting like so many termites and chewing through the framework of our fundamental rights.

If passed, this bill would be the strongest protection for Americans' privacy in a century. I need your help to tell Congress to pass our bill, and put a big win on the board for the Constitution.

Which brings me to the second point - Restoring a system that puts our rights and freedom first will take change in every part of our government: Legislation must recognize that technology should empower individuals, not the state or major corporations at the individual's expense. Courts must rule based on the original values of the constitution, not an outdated understanding of technology. And the executive branch must realize that all-encompassing surveillance of our own people, whether by the NSA, or purchased from a data broker, will leave our country weaker without making us more secure.

Achieving that vision won't be easy. And it won't be done solely by politicians in Washington, D.C. It will take a grassroots effort to make sure that those in power don't give away our rights cheaply.