Testimony of Former Congressman Bob Goodlatte
Before the House Committee on the Judiciary
Hearing on "Digital Dragnets:
Examining the Government's Access to your Personal Data"
July 19, 2022

Chairman Nadler, Ranking Member Jordan, members of the committee, thank you for this opportunity to testify.

I am honored to be back before this committee and so many of my former colleagues. Today I come to you as a private citizen and Senior Policy Advisor for the Project for Privacy & Surveillance Accountability, or PPSA. We are a nonpartisan group of U.S. citizens who advocate for greater protection of our privacy and civil liberties in government surveillance programs. We work on a daily basis with about ten other organizations across the political spectrum to protect the 4th Amendment rights of Americans.

That Amendment reads in full: "The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

A loophole that we never imagined, one as big as the J. Edgar Hoover FBI Building, has weakened the protection of Americans' privacy. Government agencies, federal, state, and local, are asserting that they can flout the Fourth Amendment's requirement for a probable cause warrant by simply buying our personal data. In effect, the government has operationalized an extraordinarily aggressive theory of law that says the government's ability to secretly buy information overwhelms Americans' Constitutionally and statutorily protected right to privacy. And so, government agencies – ranging from the Defense Intelligence Agency, to the IRS, to likely the FBI and CIA as well – are

buying or soliciting the personal data of millions of Americans they would otherwise have to go to a court to get a warrant to obtain.

When I served on the Committee, we tried to update the Electronic Communications Privacy Act, or ECPA. That law was written in 1986, a time when the main electronic threat to privacy was the extraction of emails directly from a computer or a server. The law treated a digital computer then not as a node in a global network, but essentially as the modern equivalent of a shoebox full of personal documents hidden under one's bed. We wanted to bring ECPA up to speed with the current state of technology, focusing on the "cloud" and other innovations. We labored to balance the privacy interests of American citizens against law enforcement's duty to keep us safe.

I am proud of the work we did, but we were not able to get the other house to act on our amendments. The need for reform today is even more urgent.

The richness of the information gleaned from digital sources far surpasses what could be put into a shoebox. My PPSA colleague, former Sen. Mark Udall, joined with a former Member of this Committee, Elizabeth Holtzman, to describe what is at stake in our digital privacy.

They wrote: "Our digital trails tell the stories of our lives, from dating apps to medical conditions revealed by our search queries, to religious and political beliefs, to our financial difficulties or windfalls. Like the colored dots in a pointillistic portrait, these data points compose a complete portrait of individuals."

Of the cloud, they wrote that "it's as if we allowed hordes of strangers to pass around our diaries and private financial ledgers, while trusting them not to ever take a peek."

But they do peek ... and far more than that.

Much of our data scraped from apps and social media platforms are sold as digital dossiers to private-sector data brokers. These brokers already compile portraits of us based on our race, ethnicity, religion, gender, sexual orientation, and income. They record major life events such as pregnancy, a job loss, or a divorce. These digital traces contain our location histories, where we shop, where we travel to and possibly who we meet with, which political candidates we support and causes we believe in.

In the back of our minds, we know that the “free” social media platforms and cellphone apps we use are not truly free. We always pay a cost in privacy. When Facebook knows we have a dog, it uses that information to present us with an ad for dog food.

Some are nonchalant about this – who cares if a private company knows enough about me to want to sell me dog food? Others are outraged at this invasion of our privacy by corporate entities. I would add, however, that the extraction of our personal data, in this case our location data, by the government is entirely different and far more ominous. No private party can break down your door at dawn, take you out in handcuffs, and charge you with a crime. No private party can fine you, enjoin you, restrain you, tax you and deprive you of your liberty and, yes, even your life.

Only the government can do that.

Our very country began largely out of anger and fear of what a government can do to people when it doesn’t respect their privacy. The offensiveness of seizures of Americans’ personal information by agents of the British Crown explains why the framers of the Constitution explicitly required a warrant based on probable cause before officials can examine our “persons, houses, papers, and effects.”

Now government lawyers are embellishing this work of the framers by adding, “unless we buy it!”

This practice defies the Fourth Amendment. It also defies *Carpenter v. U.S.* a 2018 Supreme Court opinion that held that the government needs a warrant to access the location history of an American extracted between cellphones and a cell tower. This practice also ignores the guidance of another Supreme Court opinion from 2014, *Riley v. California*, in which the Court determined that law enforcement cannot examine the data in a suspect's cellphone without a warrant. In a memorable phrase, the Court found a cellphone is not just a technological convenience, but a repository that holds for Americans "the privacies of life."

A reasonable interpretation of these two opinions should have prompted government lawyers to question any warrantless access to Americans' electronic data. Instead, like a flippant teenager, government lawyers take these restrictions as a sign that anything not expressly prohibited must be permissible.

Thus, Senator Ron Wyden reports that the Defense Intelligence Agency informed his office that it does not have to adhere to the Constitution or the *Carpenter* ruling when it buys data. That is outrageous.

Senator Mike Lee has said that "The Federal Government should not be allowed to skirt the Fourth Amendment's existing requirements and surveillance laws by purchasing American's data from third party brokers."

Even more outrageous is how data purchasing operates in practice.

Yesterday, the American Civil Liberties Union published revelations from its Freedom of Information Act request to the Department of Homeland Security. ACLU reports that DHS agencies are paying millions of taxpayer dollars to two data brokers to buy Americans' telephone location data. ACLU also reports that the marketing materials of one of the data brokers claims to collect more than 15 billion location points from over 250 million cell phones and other mobile devices *every day*.

The Department of Defense, for example, has used this tactic to access data from a dating app, Muslim Mingle, as well as a popular Muslim app that provides reminders for daily prayers. Imagine, this government agency managed to compromise the Fourth Amendment *and* degrade the First Amendment right to the free exercise of religion in just one move.

We don't know the extent of this practice across the government, though there is reason to be deeply alarmed. In February, Senators Wyden and Martin Heinrich revealed a finding by the Privacy and Civil Liberties Oversight Board that the CIA is engaged in bulk collection, based not on a statutory authority, but on Executive Order 12333. Although the public does not know precisely how the CIA is vacuuming up so much information, Senators Wyden and Heinrich, who both serve on the Senate Select Committee on Intelligence, tell us this mass surveillance is occurring "entirely outside the statutory framework that Congress and the public believe govern this collection, and without any of the judicial, Congressional, or even executive branch oversight that comes with FISA collection." This strongly suggests that legal acrobatics similar to the DOD's are at play.

We know that the government has the appetite for our personal information. In April, the *Wall Street Journal* reported that the FBI conducted almost 3.4 million warrantless queries of information acquired under FISA's § 702 using the identities of people inside the United States during a recent one-year period.

Many other instances of federal agencies purchasing Americans' data from private brokers have been reported, and more appear likely to be reported, if Congress does not act.

The Brennan Center for Justice reports that the FBI, Department of Homeland Security, and the Secret Service have all been caught secretly purchasing cell phone location information. It's time to put a stop to this practice which violates the Fourth Amendment.

Under current law, the government cannot obtain records from companies like Facebook and Google without a court order. Why should data brokers be treated any differently? Similarly, if the government wished to compel data brokers to deliver these records, rather than secretly buying them, it would also need to obtain a court order. The narrowness and obscurity of the loophole the government is exploiting underscore how shaky its legal foundation is.

I ask: Does this loophole make any sense to you, as students of the Constitution and the law?

The solution is, I suggest, the Fourth Amendment Is Not for Sale Act ("FANFSA"). This bill would close the loopholes in the Electronic Communications Privacy Act, as well as the Foreign Intelligence Surveillance Act that the government exploits to buy our most sensitive and personal data. Among other things FANFSA would require the government to get a court order to compel data brokers to disclose data. It would prevent law enforcement and intelligence agencies from buying data on people in the U.S. and about Americans abroad, if the data was obtained from a user's account or device or via deception, hacking, or violations of a contract, privacy policy or terms of service. Importantly, FANFSA requires intelligence agencies acquiring data on Americans do so within the framework of the Foreign Intelligence Surveillance Act and that when obtaining Americans' location data, web browsing records and search history, intelligence agencies obtain probable cause orders. This is similar to the goal of the 2020 Daines-Wyden amendment, which the Senate overwhelmingly supported to rein in § 215 of FISA.

When the Fourth Amendment Is Not for Sale Act passes, U.S. law enforcement and intelligence agencies will still have powerful legal tools at their fingertips with which to follow leads that can catch terrorists, spies, and dangerous criminals. They will just have to follow the rules.

I thank Chairman Nadler and Congresswoman Lofgren for their leadership in introducing this legislation. Senators Ron Wyden and Rand Paul have introduced it in the Senate. Ranking Member Jordan has also expressed concern about the scale of the surveillance state and its impact on individual Americans' fundamental liberties and fundamental rights. Senator Steve Daines has called for action saying: "We must close the loopholes that allow the federal government to circumvent the Fourth Amendment and buy Americans' personal data."

Respect for the rules that protect American's privacy is essential to democratic government. I commend the Chairman, the Ranking Member, and this Committee for delving into the shadowy, secretive world of data markets. The more answers you can compel from the government about the scope and uses of Americans' purchased data, the better we will be able to devise rules to protect the American people from lawless mass surveillance.

Thank you.