DAILY NEWS

Government surveillance doesn't stop at your bank's door

Jennifer J. Schulp and Norbert J. Michel

August 11th, 2022

Modern life is full of sharing mundane information with others. Your cellphone company knows where you've been, your home security system knows your visitors, and your bank knows your spending habits.

And it's often not *just* your service providers that know. Law enforcement has used many of these treasure troves of information without first obtaining a warrant. This warrantless surveillance — which prompted a recent hearing by the House Committee on the Judiciary — may be novel for technology and media companies, but it is nothing new when it comes to the government's surveillance of Americans' *financial* activity.

The Bank Secrecy Act of 1970 (BSA) requires financial institutions to assist federal agencies in detecting and preventing money laundering and other crimes. It does this in a number of ways, including by enlisting financial institutions to report certain customer activities to the government.

One report is a "currency transaction report," which is filed for any deposit, withdrawal or other transaction involving currency of more than $10,000. That means if you deposit more than $10,000 in cash, your bank must tell the government. And it's illegal to try to avoid the report by breaking a transaction into smaller increments.

Financial institutions also must file "suspicious activity reports" on transactions suspected to be related to illegal activity. The government requires these reports be kept confidential, including from the customer implicated.

These obligations don't just apply to banks; they also apply to a host of entities including currency exchanges, money transmission businesses, broker-dealers, casinos, pawnbrokers, travel agencies and car dealerships. In 2019, more than 20 million reports were filed by more than 97,000 entities.

As Rep. Jerrold Nadler put it: "The easy availability of personal data to the government poses significant risks to minorities, to those with unpopular views, to our system of justice, and ultimately, to the stability of our democracy itself." While the government's interest in stopping crime is certainly an important one, the Constitution's Fourth Amendment already balances that interest with an individual's interest in privacy by requiring the government to obtain a warrant to access a person's documents and information.

The BSA fails to achieve the Fourth Amendment's balance, and the Supreme Court is partly to blame. Several cases in the 1970s established what is known as the "third-party doctrine," which essentially exempts information that has been provided to a third party, like a bank, from the Fourth Amendment's protections. Under that doctrine, since such information is no longer "private," the government can access it from the third party.

Although the Supreme Court upheld the law's constitutionality — when the government required less reporting from financial institutions — several justices were concerned about the BSA's privacy intrusions. Two justices cautioned in California Bankers Association vs. Shulz that significantly extending the reporting requirements would be problematic, explaining that "[f]inancial transactions can reveal much about a person's activities, associations and beliefs. At some point, governmental intrusion upon these areas would implicate legitimate expectations of privacy." Other justices thought that the BSA had already crossed the constitutional line. Justice Thurgood Marshall was clear: "By compelling an otherwise unwilling bank to photocopy the checks of its customers the government has as much of a hand in seizing those checks as if it had forced a private person to break into the customer's home or office and photocopy the checks there."

The scope of the BSA's surveillance has greatly expanded since then through additional regulatory requirements and the increasing use of intermediaries in routine financial transactions. Some current Supreme Court justices, including Neil Gorsuch and Sonia Sotomayor, have recognized that today's reliance on technology requires revisiting the third-party doctrine. As Gorsuch explained, "just because you *have* to entrust a third party with your data doesn't necessarily mean that you should lose all Fourth Amendment protections in it."

Even without a Supreme Court condemnation of the BSA, though, Congress should step up to prohibit this type of government surveillance. While not without its problems, the Stored Communications Act prohibits an end-run around the Fourth Amendment for data collected by internet service providers. The bipartisan Fourth Amendment Is Not For Sale Act, introduced in the Senate, would prohibit law enforcement from purchasing individuals' data. Congress should apply the same logic to financial data.

Catching criminals is a worthy goal (even if it's questionable how much the BSA contributes to that effort), but the Fourth Amendment already balances privacy with law enforcement needs by requiring the government to get a warrant. The same rules should apply under the BSA.

Norbert J. Michel is vice president and director of the Cato Institute's Center for Monetary and Financial Alternatives.