THE EPOCH TIMES

How Government Makes Your Bank Spy on You

Kevin Stocklin

November 4, 2022

When you open a bank account, do you surrender all rights to your privacy and personal data?

Today, the answer is yes. The Bank Secrecy Act of 1970 (BSA) and subsequent amendments mandated that your bank must inform the federal government about any customer's transactions that they consider suspicious, however broadly defined that may be, in the form of Suspicious Activity Reports (SARs).

How often do banks think their customers are doing something suspicious? According to the U.S. Treasury Financial Crimes Enforcement Network, there were approximately 20 million bank reports of suspicious activity in 2019.

An August report by the Cato Institute titled "Government Surveillance Doesn't Stop at Your Bank's Door" states that this reporting requirement doesn't just apply to banks but also to currency exchanges, payments companies, broker-dealers, casinos, pawnbrokers, travel agencies, and car dealerships.

All of this would seem to be illegal under the U.S. Constitution; the Fourth Amendment, for example, prohibits "unreasonable search and seizure" by our government and establishes the requirement for the government to obtain a warrant and show "probable cause" of a crime. But according to Jennifer Schulp, co-author of the Cato report, one reason that government surveillance-by-proxy has been allowed by U.S. courts, including the U.S. Supreme Court, is something called the "Third Party Doctrine."

Schulp told The Epoch Times that the Third Party Doctrine is a legal principle that "essentially removed the expectation of privacy that an individual has from information that they share with a third party, including their banks. So under current Fourth Amendment jurisprudence, the information that you give to your bank is no longer private."

Given that it is nearly impossible to function without a bank account in America today, this effectively blurs the line between public and private surveillance. When the Third Party Doctrine was adopted in the 1960s and 1970s, the courts began to allow government to conduct warrantless searches in the interest of preventing crime.

The Cato report points out that "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."

Another reason the Supreme Court allowed the Bank Secrecy Act to stand was that the law as originally written was more narrowly tailored, and only required reporting of transactions over

$10,000. Taking inflation into account, this would be about $75,000 today. The limits of the BSA were never adjusted up for inflation, casting a much wider net today than when the law was passed.

How Extensive Is Government Surveillance?

Since being signed off on by the Supreme Court, the law has since been expanded to include many more types of transactions and institutions. But the fact that, according to the law, banks do not tell customers that they're being surveilled, means that there are few challenges for courts to take up in order to reconsider their verdict.

"Banks are not allowed to let individuals know that this type of report is being filed on them," Schulp said. "So to the extent that individual citizens might have objections to their information being shared with the government in a Suspicious Activity Report, they have no way of knowing that that's happening to them, and thus can't really bring the legal challenge themselves."

Even at the time of the BSA's original passage, some justices expressed concerns that the constitution was being violated. Justice Thurgood Marshall, for example, stated that "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."

This issue is now being raised again today not only about bank surveillance but also about tech surveillance and even tech censorship. The question is: If the government is barred from warrantless searches, can it get around this simply by getting private corporations to search Americans' data on its behalf? Likewise, if the government is barred from censoring Americans' speech, can it just get private tech companies to do this instead?

The extent of bank surveillance has made headlines this year, in three cases in particular. The first was a New York Post report that Bank of America had data-mined its customers' accounts to see which customers had made purchases or traveled to Washington, D.C., around the time of the Jan. 6 riots at the Capitol. The names of customers who had done so, or who had recently bought a firearm, were handed over to the FBI for investigation. One customer was reportedly questioned by the FBI as a result, but no charges were filed.

The second case regards a decision by credit card companies—Visa, Mastercard, and American Express, in particular—to begin tracking their customers' purchases at gun shops. The CEO of Amalgamated Bank, a progressive bank that had lobbied heavily for the tracking of gun sales, stated that "where there may be gun sales that are intended for black markets or we see patterns of gun purchases made in multiple gun shops … we can provide that information to authorities to investigate."

Gun rights advocates were quick to criticize this action.

"They've created this merchant category code that if you go into a gun store and you purchase anything from that gun store, and it looks like it may be something outside the norm, then that information could be turned over to the U.S. Treasury's Financial Crimes Enforcement

Network," Mark Oliva, public affairs director for the National Shooting Sports Foundation, told The Epoch Times. "What we're talking about with this is a heavy-handed approach that's going to put people who are exercising their Second Amendment rights onto a government watchlist, simply for exercising that right."

The third case occurred in February, when Canadian banks data-mined the private accounts of truckers protesting pandemic regulations, as well as those who had donated in support of protesters via crowdfunding sites like GoFundMe and GiveSendGo. Under orders from the Canadian government, banks froze the accounts of targeted customers, blocking them from accessing their own money or making credit card payments.

"That Third Party Doctrine has come under criticism a lot over the years, by current Supreme Court justices from very different schools of thought," Schulp said. "Justice Neil Gorsuch and Justice Sonia Sotomayor have indicated that the Third Party Doctrine needs to be revisited. So I think it's something that the current court might look at differently than the court did in the 1970s."