

» [Print](#)

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to colleagues, clients or customers, use the Reprints tool at the top of any article or visit: www.reutersreprints.com.

Exclusive: U.S. plans to let spy agencies scour Americans' finances

6:51pm EDT

By [Emily Flitter](#) and [Stella Dawson](#) and [Mark Hosenball](#)

NEW YORK/WASHINGTON (Reuters) - The Obama administration is drawing up plans to give all U.S. spy agencies full access to a massive database that contains financial data on American citizens and others who bank in the country, according to a Treasury Department document seen by Reuters.

The proposed plan represents a major step by U.S. intelligence agencies to spot and track down terrorist networks and crime syndicates by bringing together financial databanks, criminal records and military intelligence. The plan, which legal experts say is permissible under U.S. law, is nonetheless likely to trigger intense criticism from privacy advocates.

Financial institutions that operate in the United States are required by law to file reports of "suspicious customer activity," such as large money transfers or unusually structured bank accounts, to Treasury's Financial Crimes Enforcement Network (FinCEN).

The Federal Bureau of Investigation already has full access to the database. However, intelligence agencies, such as the Central Intelligence Agency and the National Security Agency, currently have to make case-by-case requests for information to FinCEN.

The Treasury plan would give spy agencies the ability to analyze more raw financial data than they have ever had before, helping them look for patterns that could reveal attack plots or criminal schemes.

The planning document, dated March 4, shows that the proposal is still in its early stages of development, and it is not known when implementation might begin.

Financial institutions file more than 15 million "suspicious activity reports" every year, according to Treasury. Banks, for instance, are required to report all personal cash transactions exceeding \$10,000, as well as suspected incidents of money laundering, loan fraud, computer hacking or counterfeiting.

"For these reports to be of value in detecting money laundering, they must be accessible to law enforcement, counter-terrorism agencies, financial regulators, and the intelligence community," said the Treasury planning document.

A Treasury spokesperson said U.S. law permits FinCEN to share information with intelligence agencies to help detect and thwart threats to national security, provided they adhere to safeguards outlined in the Bank Secrecy Act. "Law enforcement and intelligence community members with access to this information are bound by these safeguards," the spokesperson said in a statement.

Some privacy watchdogs expressed concern about the plan when Reuters outlined it to them.

A move like the FinCEN proposal "raises concerns as to whether people could find their information in a file as a potential terrorist suspect without having the appropriate predicate for that and find themselves potentially falsely accused," said Sharon Bradford Franklin, senior counsel for the Rule of Law Program at the Constitution Project, a non-profit watchdog group.

Despite these concerns, legal experts emphasize that this sharing of data is permissible under U.S. law. Specifically, banks' suspicious activity reporting requirements are dictated by a combination of the Bank Secrecy Act and the USA PATRIOT Act, which offer some privacy safeguards.

National security experts also maintain that a robust system for sharing criminal, financial and intelligence data among agencies will improve their ability to identify those who plan attacks on the United States.

"It's a war on money, war on corruption, on politically exposed persons, anti-money laundering, organized crime," said Amit Kumar, who advised the United Nations on Taliban sanctions and is a fellow at the Democratic think tank Center for National Policy.

SUSPICIOUS ACTIVITY

The Treasury document outlines a proposal to link the FinCEN database with a computer network used by U.S. defense and law enforcement agencies to share classified information called the Joint Worldwide Intelligence Communications System.

The plan calls for the Office of the Director of National Intelligence - set up after 9/11 to foster greater collaboration among intelligence agencies - to work with Treasury. The Office of the Director of National Intelligence declined to comment.

More than 25,000 financial firms - including banks, securities dealers, casinos, and money and wire transfer agencies - routinely file "suspicious activity reports" to FinCEN. The requirements for filing are so strict that banks often over-report, so they cannot be accused of failing to disclose activity that later proves questionable. This over-reporting raises the possibility that the financial details of ordinary citizens could wind up in the hands of spy agencies.

Stephen Vladeck, a professor at American University's Washington College of Law, said privacy advocates have already been pushing back against the increased data-sharing activities between government agencies that followed the September 11 attacks.

"One of the real pushes from the civil liberties community has been to move away from collection restrictions on the front end and put more limits on what the government can do once it has the information," he said.

Michael German, senior policy counsel for the American Civil Liberties Union, said that U.S. officials had floated a similar scheme to pool such data a decade ago, but that funding for the plan was later withdrawn by Congress.

He said one of the problematic aspects of the plan is that there is "wobble room" on how the information will be used. In the past, the National CounterTerrorism Center, which is supposed to ensure that critical threat information is shared among various agencies, was obliged to "promptly identify and purge any innocent U.S. person information."

But the guidelines were subsequently loosened so that "not only can they keep the data for a number of years, but they can continue to use it," German said.

Once spy agencies get such data, German said, "it's in a black hole. Time and again, we have evidence, unfortunately well after the fact, that somebody's civil rights have been violated, that the intelligence community simply ignores the rules."

(Reporting by Emily Flitter in New York, Stella Dawson and Mark Hosenball in Washington; Editing by Tiffany Wu and Leslie Gevirtz)

© Thomson Reuters 2011. All rights reserved. Users may download and print extracts of content from this website for their own personal and non-commercial use only. Republication or redistribution of Thomson Reuters content, including by framing or similar means, is expressly prohibited without the prior written consent of Thomson Reuters. Thomson Reuters and its logo are registered trademarks or trademarks of the Thomson Reuters group of companies around the world.

Thomson Reuters journalists are subject to an Editorial Handbook which requires fair presentation and disclosure of relevant interests.

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to colleagues, clients or customers, use the Reprints tool at the top of any article or visit: www.reutersreprints.com.

