THE WALL STREET JOURNAL.

EU Leans Heavily on U.S. Program Tracking Terror Financing

Even while faulting U.S. privacy protections, Europeans use data gathered

Byron Tau | November 19, 2020

The U.S. has shared Terrorist Finance Tracking Program data with European partners about a number of serious terrorist incidents in Europe—including a 2017 truck attack in Stockholm.

WASHINGTON—A new review by a civil-liberties watchdog has revealed the extent to which European governments have come to rely on a U.S. surveillance program that monitors global financial transactions for ties to terrorism.

The Treasury Department's Terrorist Finance Tracking Program, or TFTP, was created after the Sept. 11, 2001 attacks. New data shows it is now widely used by European authorities—even as European Union institutions, concerned about the privacy of their citizens and possible surveillance, move to more strictly control transfers to the U.S. of data they gather.

Some 40% of the database searches performed by Treasury were on behalf of EU member states or Europol, the EU's law-enforcement arm, according to information gathered as part of a review by the U.S. Privacy and Civil Liberties Oversight Board, an independent federal agency that advises the president on intelligence and counterterrorism programs.

As a result of the audit, which covered three years, the board submitted classified recommendations to improve the program while its chairman, Adam Klein, issued a statement offering new details about the extent of U.S.-EU cooperation on counterterrorism efforts.

Both sides of the Atlantic are grappling with the future of data sharing between the U.S. and Europe.

Mr. Klein revealed that in one 35-month period examined by the board—Jan. 2016 to Nov. 2018—some 80,000 leads were shared with European authorities. Nearly 75% of all disseminations shared with foreign governments under TFTP have been with EU member states or institutions.

The program, "though funded and operated by the United States, provides a steady stream of valuable intelligence to EU member states," Mr. Klein said. "That should be welcome news to every American."

Much of the data queried by Treasury actually originates in Europe with a Belgian firm known by its acronym, Swift, which facilitates most of the world's interbank messaging. A 2010 EU-U.S. agreement governs U.S. access to any Swift data stored in Europe for the purposes of counterterrorism.

Europol, the EU's law-enforcement arm, is a significant beneficiary of database searches conducted by the U.S. Terrorist Finance Tracking Program.

But EU member states and EU law-enforcement units also are able to request and use intelligence generated from the Swift network, passing its requests through the U.S. for searching and processing—bypassing the need for a European version of the program and relying on the U.S. to conduct sensitive and controversial searches of European data. The Treasury Department then uses its access to Swift data to run searches on behalf of European allies.

"The EU has effectively deputized the U.S. Treasury to perform counterterrorism searches of European data," said Mr. Klein.

The U.S. has shared TFTP data with European partners about a number of serious terrorist attacks in Europe—including the 2017 truck attacks in Barcelona and Stockholm, the November 2015 Paris attacks by Islamic radicals and the 2011 mass shooting by right-wing terrorist Anders Breivik in Norway, according to the Treasury Department.

The program has been controversial in Europe from the start. A number of lawmakers in the EU Parliament or within member state governments have called for it to be scrapped. Privacy activists have pushed for curtailing all types of data transfers to the U.S., which they claim doesn't offer adequate privacy protections.

Under the U.S.-EU agreement governing the program, European overseers monitor the TFTP for compliance with EU regulations. One is appointed by Swift, the other is appointed by the European Commission. Swift also appoints an external auditing firm to review the program.

In general, the EU has much stricter rules governing personal data privacy. An EU effort to create its own version of TFTP has floundered, with one top official concluding in 2013 that it faced "serious challenges in terms of the data storage, access and protection."

A spokeswoman for the EU mission to the U.S. didn't respond to a request for comment.

The U.S. and EU have been wrangling over issues related to international data transfers for years with European regulators, parliamentarians and courts complaining that there are inadequate privacy protections in U.S. law for data queried for intelligence purposes.

The latest twist came in July, when the European Court of Justice in a surprise ruling invalidated a widely used EU-U.S. data-transfer agreement known as Privacy Shield. The court ruled that the structure of U.S. intelligence programs left Europeans citizens vulnerable to American government surveillance without "actionable rights" to challenge such surveillance in court.

The ruling didn't affect TFTP, which is governed by a different separate EU-U.S. agreement, though the program and data-transfer issues broadly have long been one of the most difficult issues between Europe and the U.S.

The existence of the TFTP, a secret program, was revealed in 2006 by three newspapers, including The Wall Street Journal. U.S. officials at the time called the disclosures "regrettable."

In the years since then, the program's existence has been declassified and debated openly on both sides of the Atlantic.