US PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

November 19, 2020

Statement by Chairman Adam Klein on the Terrorist Finance Tracking Program

I am grateful to the staff members whose diligent, skillful work has brought the Board's review of the Terrorist Finance Tracking Program, or TFTP, to a successful conclusion. The Board's review indicates that TFTP is thoughtfully designed, provides significant value for counterterrorism, and appropriately protects individual privacy. The recommendations provided to the Department of the Treasury, which administers TFTP, will reinforce the program's privacy safeguards.
I write separately to highlight one important aspect of TFTP: the respective roles of the United States and European Union in the program's design, implementation, and use in countering terrorism.

Since the Second World War, our alliance with the democratic nations of Europe has been the fulcrum of America's global security posture. Intelligence and counterterrorism cooperation, though less visible than the NATO military pact, form an important part of this transatlantic partnership.

The United States spends around $60 billion each year on intelligence programs, not including purely military activities.[1] Many of those programs produce significant benefits for European allies, in addition to unilateral benefits for the United States. For example, U.S. agencies frequently share valuable intelligence produced under Section 702 of the Foreign Intelligence Surveillance Act with their European counterparts.[2] The regularity and volume of our intelligence sharing with Europe reflects a ground truth of postwar American strategy: only a strong Atlantic alliance based on shared values, interests, and burdens can ensure a world that is hospitable for our way of life.

TFTP fits squarely within this tradition of security cooperation. With respect to European data, TFTP resembles an outsourcing arrangement, with the U.S. Treasury Department effectively serving as an offshore service provider for the EU and European governments.

---

[1] *See* Office of the Director of National Intelligence, U.S. Intelligence Community Budget, *at* https://www.dni.gov/index.php/what-we-do/ic-budget ("top-line" budget data back to 2006). For Fiscal Year 2020, the total amount requested for the National Intelligence Program was $62.8 billion. Office of the Director of National Intelligence, *DNI Releases Budget Figure for FY 2020 Appropriations Requested for the National Intelligence Program* (Mar. 18, 2019).
[2] The U.S. government has released unclassified descriptions of several cases in which NSA shared critical counterterrorism intelligence derived from Section 702 with European partners. *See* NSA/CSS, *"Section 702" Saves Lives, Protects the Nation and Allies* (Dec. 12, 2017); Office of the Director of National Intelligence, *Guide to Section 702 Value Examples* (Dec. 4, 2017).

Understanding how this works requires a bit of background on the Society for Worldwide Interbank Financial Telecommunication, or SWIFT. SWIFT is a non-profit cooperative that provides secure global financial messaging services to banks and other financial institutions. SWIFT, which is based in Belgium, transmits millions of messages each day for its customers. Where those messages are stored depends on where each customer is located.

Data for bank customers located in EU countries is assigned to SWIFT's European Zone and stored in operations centers in the Netherlands and Switzerland. Normally, that data would stay in Europe. TFTP, however, creates an exception to that rule: Under the U.S.-EU agreement that governs TFTP, SWIFT provides certain data located in its European data centers to the U.S. Treasury.[3]

The EU Agency for Law Enforcement Cooperation, or Europol, then sends terrorism-related search requests to Treasury. Treasury runs those searches against the TFTP data and sends the results back to Europol, which distributes them to European governments. Treasury also sends some TFTP leads directly to European governments.

Treasury's exertions on behalf of European counterparts are far from a minor aspect of the program. Indeed, a significant proportion of all TFTP searches are run on behalf of European partners. Specifically, during the thirty-five months covered by the last EU review of TFTP, more than 40% of the total number of searches were run in response to requests from Europol or EU member states.

Of all foreign recipients, the EU and its member states receive by far the largest number of TFTP disseminations. From the program's inception through 2019, the EU received more than 2,750 reports from TFTP—nearly three-quarters of all foreign disseminations.[4] Sharing with the EU is also faster: Treasury provides "expedited dissemination" of lead information to Europol.

Many of the useful leads generated by TFTP relate to terrorist threats to European Union member states. From January 2016 to November 2018, Treasury shared more than 80,000 individual leads from TFTP with EU authorities and member-state governments.[5]

TFTP leads have been shared in response to many of the most infamous attacks and plots against European countries in recent memory.[6] Unclassified examples include:

- 2017: Stabbing attack in Turku, Finland
- 2017: Attacks in and around Barcelona
- 2017: Truck attack in Stockholm

[3] Data related to the Single Euro Payments Area, or SEPA, is excluded.
[4] European Commission, *Commission Staff Working Document accompanying the Report from the Commission to the European Parliament and the Council on the Joint Review of the Implementation of TFTP*, at 25 (July 22, 2019).
[5] Reports often contain more than one lead.
[6] TFTP leads were also shared in response to terrorist attacks outside of Europe, including the 2010 Nigerian Independence Day car bombings in Abuja, the 2009 hotel attacks in Jakarta, the 2008 terrorist attacks in Mumbai, and the 2002 bombings in Bali.

- 2015: Attacks in Paris and raid in Saint-Denis
- 2015: Attack in Paris and anti-terrorism raid in Verviers
- 2012: Threats to London Summer Olympic games
- 2011: Attacks in Norway conducted by Anders Breivik
- 2009: Hijacking of the Belgian vessel MV Pompei
- 2007: Islamic Jihad Union plot to attack sites in Germany
- 2005: Bombings in London
- 2004: Van Gogh terrorist-related murder in the Netherlands
- 2004: Madrid train bombings

The response to the horrific Breivik attacks in Norway is illustrative. In that case, "TFTP-based information helped Norwegian and other European investigators including Europol to, within hours, identify the channels through which Breivik collected and moved the funds used for the preparation of his vicious attacks."[7] Based on the TFTP data from the Breivik case, "Finnish authorities were able to arrest a person pursuing similar terrorist objectives before he was able to put them into practice."[8]

The sharing continues. A Europol memo documents additional instances in recent years in which TFTP helped authorities in EU member states track financial flows to terrorist groups.
The bottom line is that this program, though funded and operated by the United States, provides a steady stream of valuable intelligence to EU member states. That should be welcome news to every American. Helping our European allies defend their citizens' safety and way of life advances our mutual interests and honors our shared values.

At the same time, EU officials have repeatedly raised concerns about TFTP's privacy protections. Some members of the European Parliament have called for TFTP to be scrapped.
Privacy questions surrounding TFTP are legitimate and important. Our Board chose to conduct a multi-year review of this program because we agree that this type of collection requires robust privacy safeguards.

The problem is that the tenor and direction of these criticisms might suggest to an untutored observer that TFTP is a unilateral American project. Perhaps the United States has inadvertently fostered that misperception by serving as the visible lead partner while European participants remain in the background.

It did not have to be that way. The 2010 U.S.-EU Agreement on TFTP provided that the European Commission would study "the possible introduction of an equivalent EU system allowing for a more targeted transfer of data."[9]

---

[7] European Commission, Press Release, *Terrorist Finance Tracking: Citizen's Safeguards Are in Place* (Dec. 14, 2012).
[8] *Id.*
[9] Alternatively, some European officials have proposed creating an EU system to complement rather than replace TFTP. *See* Mara Wesseling, Royal United Services Institute for Defence and Security Studies, *An EU Terrorist Finance Tracking System* 14-17

Instead of sending European SWIFT data to the U.S. to be searched by our Treasury Department, the EU would explore whether to create its own version of TFTP, which would keep the data in Europe.

That European version of TFTP never made it to the drawing board. In 2013, the EU Commissioner for Home Affairs concluded that it "would be expensive and demanding on resources to put in place and maintain."[10] She found that it would "require the creation of a gigantic database containing data of EU citizens' financial transfers. Such [a] database would raise serious challenges in terms of the data storage, access and protection, not to mention the huge technical and financial efforts."[11]

Put simply, the EU found that a replacement for TFTP would be costly and difficult to build, maintain, and secure. (Even assuming that a replacement would produce as much useful intelligence as the original.)

There may also be other, less obvious reasons for some Europeans to prefer things as they are. The present arrangement pretermits thorny questions about EU bodies' involvement in national security, traditionally the domain of member states. It circumvents the difficult task of harmonizing rules across 27 different legal systems. It avoids potentially awkward issues of trust and precedence among member states. And it inclines privacy activists, Data Protection Authorities, and parliamentarians to focus their concerns on the United States, rather than Europol or whatever entity would operate a European version of TFTP.[12]

In this light, it becomes less perplexing that the EU has effectively deputized the U.S. Treasury to perform counterterrorism searches of European data. The present arrangement yields timely, actionable intelligence for European security services while avoiding many complications that would arise from collecting and analyzing this data in Europe.

Our Board was created because Congress believed that independent scrutiny helps ensure an appropriate balance between security and privacy. Outside scrutiny can help too, if it is fact-based and fair-minded. Unfortunately, transatlantic discussions of intelligence programs and privacy protections often omit important aspects of the U.S. system, the practices and laws of EU member states, and the ways in which both sides cooperate to protect their citizens. The regrettable demise of the U.S.-EU Privacy Shield is only the latest example.

Transatlantic discussions about surveillance and privacy could be improved by greater candor about what each side is doing, and why. Ultimately, Americans and Europeans face the same challenge: protecting our societies in a manner consistent with fundamental values and the rule of law. Respectful, candid discussion of these issues can help both sides do that better.

(Sept. 2016). An EU-run complement to TFTP could cover data from the Single European Payments Area (SEPA), which is excluded from TFTP. Were such a system in place, European analysts could search for leads in the SEPA data and share them with U.S. counterparts, much as U.S. analysts share TFTP leads with European colleagues. As of this writing, however, there does not appear to be an active effort to create such a system.

[10] Cecilia Malmstrom, EU Commissioner for Home Affairs, Remarks on European Commission Reports on TFTP and PNR (Nov. 27, 2013).

[11] *Id.*

[12] *See* Wesseling, *supra* note 9, at 23-24.