CENTER FOR DEMOCRACY & TECHNOLOGY

March 20, 2017

Section 702 and the E.U.-U.S. Privacy Shield

The E.U.-U.S. Privacy Shield agreement assists in the free flow of commerce by allowing companies to transfer data between the European Union and the United States, but it could be in jeopardy if U.S. surveillance law is not reformed. The Privacy Shield agreement was built on assurances that the U.S. would not subject Europeans' data to "indiscriminate mass surveillance." However, under Section 702 of the Foreign Intelligence Surveillance Act (FISA), the U.S. government is authorized to collect non-U.S. persons' electronic communications either stored by U.S. providers or in transit to them. Concern about this broad collection under 702 played an important role in the Court of Justice of the European Union (CJEU)'s decision to invalidate Privacy Shield's predecessor, the E.U.-U.S. Safe Harbour agreement and undergirds two current legal challenges to Privacy Shield. To ensure the continuation Privacy Shield, any re-authorization of 702 this year must be accompanied by meaningful reforms to better protect the privacy rights of non-U.S. persons.

How does Section 702 impact Privacy Shield?

- **702 played an important role in the failure of Privacy Shield's predecessor:** When the 702 PRISM program was revealed by Edward Snowden in 2013, the European Commission launched a review of the E.U-U.S. Safe Harbour. The CJEU eventually invalidated the Safe Harbour, holding that surveillance must be "necessary and proportionate" to national security needs.
- **Privacy Shield facilitates vital data transfer:** The Privacy Shield agreement allows the transfer of data between the European Union and the United States. The ability to transfer data across borders is vital to global commerce and communications networks. Privacy Shield replaced the E.U.-U.S. Safe Harbour agreement, which was invalidated by the CJEU in 2015 for failing to adequately protect Europeans' privacy.
- **The U.S. must protect Europeans' privacy:** In order for U.S. companies to transfer Europeans' data, the U.S. must provide privacy protections that are "essentially equivalent" to those provided by the E.U. The Privacy Shield agreement was reached in part because of assurances by the U.S. Director of National Intelligence that the U.S. would not subject European data to "indiscriminate mass surveillance."
- **Section 702 authorizes broad collection of Europeans' communications far beyond terrorism investigations:** Section 702 is commonly described as necessary to prevent terrorism, but it permits surveillance for other purposes as well. For example, the government can conduct 702 surveillance for the broad purpose of collecting communications relating to the "foreign affairs" or "national defense" of the United States. This could include the communications of human rights organizations, protesters, and the news media-individuals who are not suspected of any wrongdoing.
- **While Section 702 is a 'targeted' surveillance statute, it authorizes expansive collection with little outside review:** The NSA can collect all communications to, from, or about any non-U.S. person identifier (such as an email address) that is designated as a target. But there were over 106,000 targets last year, none of which were approved by a court. This high number of targets that could be surveilled for such vague purposes argues against the program being "necessary and proportionate."
- **Privacy Shield faces two legal challenges so far:** Privacy Shield currently faces two legal challenges, and the breadth of surveillance under Section 702 could play an important role in those decisions. If Section 702 is re-authorized without meaningful reforms to protect Europeans' privacy, it would mitigate in favor of striking down Privacy Shield.
- **To save privacy shield, the scope of collection under Section 702 must be narrowed so that it does not sweep in the communications of Europeans who are not foreign targets.**

For more information, visit our Section 702 issue page or contact Michelle Richardson, CDT's Deputy Director of the Freedom, Security & Technology Project, at mrichardson@cdt.org.