CRS Reports & Analysis

Legal Sidebar

UPDATE: The Microsoft Ireland Decision: U.S. Appeals Court Rules that ECPA Does Not Require Internet Service Providers To Produce Electronic Communications Stored Overseas

06/28/2017

Update 6/28/17: On June 23, 2017, the United States filed a petition for writ of certiorari in the Supreme Court requesting reversal of the Second Circuit's decision, discussed below.

Update 1/24/2017: The Second Circuit declined to rehear en banc *the panel's July 14, 2016 decision that the United States could not enforce a subpoena seeking Microsoft's emails stored on a server in Ireland. The Second Circuit voted 4-4 on the request for a full-bench rehearing, but a majority vote of the court is required. Each of the four dissenting judges authored a separate opinion, and three judges recused themselves.*

The original post from September 12, 2016, is below.

On July 14, 2016, a panel of the United States Court of Appeals for the Second Circuit unanimously ruled that the United States government could not enforce a subpoena seeking Microsoft to retrieve emails stored on a server in Ireland. The case, *Microsoft Corporation v. United States*, could have important implications both for federal law enforcement efforts to obtain electronic communications stored overseas and privacy protections afforded to those communications.

In what is commonly referred to as the Microsoft Ireland decision, the Second Circuit analyzed the jurisdictional reach of the Stored Communications Act, which was enacted in 1986 as Title II of the broader Electronic Communications Privacy Act (ECPA). Discussed in an earlier CRS Report, ECPA is the primary federal law dictating the methods the government may use to access stored electronic communications. The Microsoft Ireland case hinged on whether a particular provision of the Stored Communications Act, Section 2703, applied extraterritorially such that it allowed the government to obtain electronic communications stored outside the territorial jurisdiction of the United States.

Section 2703 establishes the conditions under which the government can require an Internet Service Provider (ISP) (in ECPA parlance, an "electronic communication service") to disclose the contents of stored communications. Basic subscriber and transactional information can be obtained with an administrative subpoena issued by certain federal agencies. But to obtain the content of electronic communications, the government must first secure a warrant under Rule 41 of the Federal Rules of Criminal Procedure or the applicable state court procedures (unless the communication is more than 180 days old and the government provides notice to the target of the warrant.)

During a criminal narcotics investigation in December 2013, federal law enforcement sought a warrant for the production of both the content of the electronic communications and certain non-content subscriber information associated with a Microsoft email account. After a federal magistrate judge granted the government's request, Microsoft complied with the portion of the warrant seeking non-content subscriber data, which was stored on servers inside the United States, but it refused to disclose the content of the email communications that was stored on servers located in

Dublin, Ireland.

According to the Second Circuit's opinion, Microsoft stores the data associated with the content of its users' email on more than 100 discrete datacenters spread over 40 countries. When an account is created, the user self-selects a "country code," and Microsoft stores the email content associated with the account in the datacenter nearest to the country that the user identified. Microsoft does not, however, verify that the user is physically located in the country that it chose.

Believing that Section 2703 does not apply extraterritorially or require it to produce data contained on a foreign server, Microsoft moved to quash the portion of the warrant seeking email content information stored in Ireland. The district court denied that motion, and, in an opinion discussed in an earlier Sidebar, held that ISPs must produce information within their control, regardless of where it is located. When Microsoft still refused to comply, the district court held it in civil contempt, and the appeal ensued. Nearly three years later, and after a host of amici briefs, the Second Circuit reversed the district court, holding that "§ 2703 of the Stored Communications Act does not authorize courts to issue and enforce against U.S.-based service providers warrants for the seizure of customer email stored exclusively on a foreign server."

Much of the Second Circuit's decision turned on whether Section 2703 authorizes warrants similar to those used in the traditional law enforcement context (Microsoft's argument) or whether it should be understood to create a process of "compelled disclosure" more akin to a subpoena (the government's position). According to the Second Circuit, warrants are not effective outside the territorial limits of the United States. Courts routinely recognize that the recipients of subpoenas, on the other hand, must produce material to the government no matter it is located, so long as it is in the recipients' custody or control. The Second Circuit ultimately concluded that "Microsoft has the better of the argument[,]" and the territorial limitations on traditional warrants applied.

Citing two recent decisions from the Supreme Court—*Morrison v. National Australia Bank, Ltd.* and *RJR Nabisco, Inc. v. European Community*—the Second Circuit stated that it was bound to apply the "strong and binding" presumption against extraterritoriality, in which, absent a clearly expressed congressional intent to the contrary, federal laws must be interpreted to have only domestic application. Using a plain meaning approach to statutory interpretation, the court highlighted that 2703 requires production of electronic communications "only pursuant to a warrant . . . ." Although the Stored Communication Act itself does not expressly touch on extraterritoriality, the court interpreted the use of the term "warrant" as evidence of Congress' intent to apply the same heightened privacy protections traditionally utilized in the warrant-seeking process to the disclosure of electronic communications. And when analyzing the legislative history, the Second Circuit concluded that the Stored Communications Act and its broader ECPA framework were focused on protecting basic privacy safeguards rather than alleviating government searches and seizures established under the Fourth Amendment.

Although some, including Microsoft, touted the decision as victory for individual privacy rights, Judge Gerard Lynch disagreed with that interpretation in a separate concurring opinion. Judge Lynch emphasized that, because the government had already satisfied the Fourth Amendment's traditional privacy protection mandate—the probable cause standard—when it obtained the warrant from a magistrate judge, the case was "not actually about the need to enhance privacy protections[,]" and was better understood as a dispute about the international reach of U.S. law.

The Microsoft Ireland decision may force federal officials seeking electronic communications stored overseas to utilize the process defined in the United States' Mutual Legal Assistance Treaties (MLATs) with foreign nations. The U.S. does not have an MLAT with every country, and the MLAT process is often criticized as slow and inadequate for the modern environment of cross-border information flow. Legislative proposals specifically addressing these issues and the "public safety implications" of the Microsoft Ireland decision are expected to be submitted by the executive branch, according to a letter from the Department of Justice (DOJ).

Other bills, such as the Law Enforcement Access to Data Stored Abroad (LEADS) Act, have been introduced to clarify the rights of government to access data stored abroad. The Microsoft Ireland decision may also impact—and possibly create further impetus for—consideration of legislation proposed by DOJ authorizing a U.S.-U.K. cross-border data-sharing agreement.