Congressional Research Service
Informing the legislative debate since 1914

Legal Sidebar

Supreme Court to Hear Digital Privacy Case: Can the Government Obtain Emails Stored Abroad?

Updated February 23, 2018

Update: In United States v. Microsoft Corp.*, the Supreme Court was set to address whether a warrant issued under the Stored Communications Act (SCA) allowed U.S. law enforcement to compel Microsoft to hand over emails it stores on a server overseas. Following the publication of this Sidebar, and less than one month after the Court heard oral argument in* Microsoft*, Congress passed and the President signed into law the Clarifying Lawful Overseas Use of Data (CLOUD) Act as part of the Consolidated Appropriations Act, 2018. The CLOUD Act amended the SCA to require that technology companies provide data in their possession, custody, or control in response to an SCA warrant—regardless of whether the data is located in the United States. The government then obtained a new warrant pursuant to the CLOUD Act and the Supreme Court dismissed the case as moot. A CRS Report providing a fuller discussion of the CLOUD Act's effect on cross-border data sharing is forthcoming.*

The original Sidebar post previewing the Microsoft case, published on February 23, 2018, is below.

Can U.S. law enforcement use a warrant to compel Microsoft to hand over emails it stores on a server in Ireland? The Supreme Court may soon answer that question in a case, *United States v. Microsoft,* that could have major repercussions for both digital privacy rights and law enforcement interests. The case comes on appeal from a 2016 decision by the U.S. Court of Appeals for the Second Circuit (Second Circuit), discussed in a previous Legal Sidebar, which held that the government could not use the Stored Communications Act (SCA) to compel Microsoft to disclose emails it stored abroad. While both the government and Microsoft agree that the SCA does not apply overseas, the central disagreement before the Supreme Court is whether using the SCA to allow the government to access electronic communications held by a domestic entity but stored abroad would constitute a domestic or foreign application of the law. This Legal Sidebar provides background on the case, including an overview of the SCA, discusses the specific issues presented by the *Microsoft* case, and explores the case's implications for Congress.

Congressional Research Service
https://crsreports.congress.gov
LSB10086

The Stored Communications Act and Extraterritoriality

Enacted in 1986, the SCA governs when and how a provider of electronic communications or remote computing services may disclose communications it stores. The statute generally prohibits providers of electronic communications from disclosing those communications to third parties. However, in a provision at issue in *Microsoft,* the statute requires disclosure to the government pursuant to a warrant based on probable cause that the communications contain evidence of a crime. Importantly, the SCA is silent on whether the law applies only in the United States or globally.

That silence is significant because longstanding precedent establishes a presumption that United States laws do not have any effect outside the country unless they specify otherwise. This interpretive rule of thumb protects against unintended conflicts between American and foreign laws that could lead to unnecessary international incidents. When this presumption applies, a critical question for courts then becomes whether a law meant only for the territorial United States is impermissibly being applied abroad or whether the law's application is appropriately domestic in nature.

Prior Supreme Court cases have laid out the test for whether an application of a law is domestic or extraterritorial: courts must look to the "'focus' of congressional concern"—what conduct the law regulates and who the law protects. The Supreme Court has explained that "[i]f the conduct relevant to the statute's focus occurred in the United States, then the case involves a permissible domestic application even if other conduct occurred abroad; but if the conduct relevant to the focus occurred in a foreign country, then the case involves an impermissible extraterritorial application regardless of any other conduct that occurred in U. S. territory." The Supreme Court has not, however, addressed what the "focus of congressional concern" was with regard to the SCA.

United States v. Microsoft

In this vein, the *Microsoft* litigation centers on whether a particular application of the SCA is impermissibly extraterritorial in nature. The case results from how Microsoft stores its customers' emails as part of its web-based email service. The company stores each individual user's emails in one of its many datacenters around the world—generally the one closest to where a user states that she is from when she signs up for the service. This case began when the government suspected that a user of Microsoft's service had communicated about illegal drug trafficking over email. The government obtained a warrant for the emails in the usual way: by satisfying a magistrate judge that there was probable cause that a crime had been committed and that the emails hosted by Microsoft were evidence of that crime. It then served the warrant on Microsoft and demanded the emails and related information.

While Microsoft complied with the warrant as to the metadata about the user that it stored on its servers located in the United States, it refused to turn over the contents of the emails, which are stored on a Microsoft server in Dublin, Ireland. Microsoft admits that it has the ability to access the emails from its U.S. computers, but contends that the SCA does not extend extraterritorially and, therefore, does not authorize the government to obtain emails that are housed on servers overseas.

The government and Microsoft agree that the SCA does not apply extraterritorially. However, they disagree over what the "focus" of the SCA is and therefore over whether this is a case that involves an impermissible extraterritorial application of that law. The government argues that the focus of the relevant provision of the SCA is on *disclosures* of electronic communications. Because the disclosure in this case would occur in the United States when Microsoft gives the emails to the government, the government maintains that this case presents a permissible domestic application of the law. In other words, for the government, the location of the emails is irrelevant because disclosure, as opposed to access to information by a provider, is at the heart of the SCA. The government further argues that even if the focus of the SCA is on user privacy, any privacy invasion occurs when the data is transferred to the government in the United States, not when the information is first transferred from abroad.

Microsoft contends instead that the focus of the SCA should be inferred from the statute's overall structure, not just the single provision that allows the government to require disclosures in certain circumstances. Microsoft thus argues, in line with the Second Circuit's holding, that the statute's focus is on the security of communications in domestic electronic storage. Because the company would have to retrieve emails stored in Ireland to comply with the warrant, Microsoft argues that the government's warrant is a result of an impermissible extraterritorial application of the law.

Ramifications and Issues for Congress

The ultimate ruling in *Microsoft* will likely be important regardless of which side prevails. A decision affirming the Second Circuit would likely make it more difficult for federal or state prosecutors to access electronic communications held by American companies if those communications are stored abroad. As the government notes, under Microsoft's theory a domestic company could even avoid complying with the SCA entirely by moving all of its servers overseas. If the government cannot use the SCA to obtain communications stored on servers in foreign countries, it would likely have to resort to processes defined in Mutual Legal Assistance Treaties (MLATs), which generally enable multinational cooperative law enforcement activities. However, the United States has MLATs with fewer than half of the nations of the world (though it does with Ireland), and the process has been criticized as "antiquated and slow." Some scholars have suggested that a ruling for Microsoft could encourage efforts to streamline the MLAT process and incentivize the execution of such treaties with more nations.

On the other hand, Microsoft argues that a ruling for the government that would allow U.S. law enforcement to access communications stored overseas could potentially create conflicts for service providers because many other nations regulate when and under what circumstances data stored within their borders can be transmitted to other countries. The European Union (EU), for example, filed an amicus brief laying out the basic contours of EU laws governing the transfer of personal data to non-EU states, which are quite stringent. Some companies argue conflicts could arise between U.S. and foreign law that would necessitate a violation of the laws of at least one of the jurisdictions the companies are subject to if the government prevails in this case. A win for the government might also embolden other countries to attempt to seize data stored here: Microsoft's brief poses the hypothetical of a Chinese warrant demanding disclosure of a journalist's emails from a U.S. server, and also points to the testimony of the company's president and chief legal officer before the House Judiciary Committee regarding real-world conflicts that have arisen in recent years from Brazil attempting to unilaterally force Microsoft to disclose emails the company stores in the United States.

Two Senators and three Representatives have filed an amicus brief in *Microsoft,* arguing that because "Congress did not intend or expect the SCA to authorize the seizure of data held within the territory of a foreign, sovereign nation," the Second Circuit's decision should be affirmed and Congress should be allowed to determine the answer to this issue legislatively. To that end, they, along with other cosponsors, have introduced the Clarifying Lawful Overseas Use of Data (CLOUD) Act—S. 2383; H.R. 4943—an amendment to the SCA that potentially could moot the *Microsoft* case by specifying how communications stored abroad may be accessed by domestic law enforcement. (The CLOUD Act would also set up a regime for allowing foreign governments to access communications stored in the U.S. in certain circumstances.) The CLOUD Act is an extension of the earlier proposed International Communications Privacy Act—S. 1671; H.R. 3718—discussed in the amicus brief.

Beyond the specific question at issue in *Microsoft*, the SCA has more broadly been the subject of criticism, with one leading commentator describing the Act as "dense and confusing." Because the SCA is structured around the state of technology as it existed in the mid-1980s, as the *Microsoft* litigation demonstrates, applying the law to modern situations can be fairly difficult. As this CRS report notes, Members of Congress have proposed various efforts to update the 1986 law in recent years. The

Supreme Court's decision in *Microsoft* may clarify the international scope of the SCA and, with that, could inform the extent to which Congress may decide to amend the law.

Author Information

Austin D. Smith
Legislative Attorney

Disclaimer