HERBERT SMITH FREEHILLS

US COURT RULING PROHIBITS US GOVERNMENT SEIZURE OF E-MAILS STORED OUTSIDE THE UNITED STATES

New York
Legal Briefings

A federal appeals court handed a major win to Microsoft when it ruled that US authorities cannot compel US tech companies to disclose e-mail content that they store on servers located outside the United States.

The case arises from Microsoft's refusal to comply with a warrant obtained by US law enforcement authorities seeking production of Microsoft customer e-mails stored on servers maintained by Microsoft's affiliate in Ireland. In a highly-anticipated decision, issued July 14, 2016, the US Court of Appeals for the Second Circuit ruled that the long-standing limitation of US warrants to searches and seizures of information located in the United States applies equally to data stored in the "cloud." Therefore, the court found that the data stored in Ireland was beyond the reach of US law enforcement authorities. See In re Warrant to Search a *Certain Email Account Controlled & Maintained by Microsoft Corp*., Case No. 14-2985 (2d Circuit July 14, 2016).

BACKGROUND

The court's decision focused on the US Stored Communications Act ("SCA"), which was enacted as part of the Electronic Communications Privacy Act in 1986, well before the advent of ubiquitous e-mail traffic, Internet use and cloud storage.

Summarized briefly, the statute prohibits Internet service providers from disclosing the contents of e-mails and other stored communications subject to certain enumerated exceptions (such as customer consent, or in an emergency situation involving serious injury or death). In the same breath, the SCA establishes a framework by which a US federal or state government entity can secure disclosure of customer data from providers. Certain information, such as basic subscriber data and other non-content information, can be obtained by means of a subpoena (an instrument requiring the recipient to turn over data within its possession, custody or control), or via court order.

The contents of e-mails, however, generally can only be obtained via a search warrant, which authorizes the government to search for and seize evidence held at an identified location. A search warrant requires the government to meet a fairly high standard: "probable cause" that a particular account contains evidence of or related to a crime. Under well-established US law, a warrant empowers the government to search for and seize evidence located within the United States, but it does not have extraterritorial application—meaning that US law enforcement can lawfully seize evidence located in Dublin, Ohio, but not Dublin, Ireland.

Against this legislative backdrop, the US government applied for and a federal magistrate judge issued an SCA warrant to seize the contents of an e-mail account belonging to one of Microsoft's customers, in connection with what is believed to be a drug-trafficking investigation. Microsoft moved to vacate the warrant insofar as the government sought e-mail content stored outside the United States. The same magistrate judge that approved the warrant also denied Microsoft's motion, and in so holding, combined the requirements surrounding the issuance and effect of a warrant with those relevant to a subpoena. Microsoft appealed to the federal district court, which, in a bench ruling, adopted and affirmed the magistrate judge's decision. The appeal to the Second Circuit followed.

THE SECOND CIRCUIT'S DECISION—SCA WARRANTS DO NOT PERMIT SEIZURE OF E-MAIL CONTENT STORED ABROAD

The Second Circuit described the case as a dispute between Microsoft and the US government regarding the "nature and reach" of the SCA warrant and the extent of Microsoft’s obligations in response to that warrant. The court noted that the SCA refers to the government's use of a "warrant" to secure content information. Warrants, however, "traditionally carry territorial limitations: United States law enforcement officers may be directed by a court-issued warrant to seize items at locations in the United States and in United States-controlled areas ... but their authority generally does not extend further."

For its part, the government sought to characterize the dispute as merely involving "compelled disclosure" of information that was in Microsoft's custody or control. It argued that similar to a subpoena, an SCA warrant requires the recipient to deliver records, physical objects, and other materials to the government "no matter where those documents are located, so long as they are subject to the recipient's custody or control." In the government's view, no extraterritoriality issues were implicated in this case, because the warrant was served on Microsoft in the US and simply called for Microsoft to retrieve the account data from its offices in the US. To support its position, the government pointed to prior cases that construed subpoenas as imposing upon their recipients the obligation to produce responsive information without regard to where a document might be located.

The Second Circuit sided with Microsoft. The court found, initially, that while the SCA prescribes the methods by which the government may obtain access to content information for law enforcement purposes, "it does so in the context of a primary emphasis on protecting user content." In other words, the SCA's aim was to protect user privacy "in the context of new technology that required a user's interaction with a service."

Having determined that the SCA focuses on customer privacy, the court had "little trouble" concluding that the execution of the warrant in this case constituted an unlawful extraterritorial application of the SCA. It noted:

"The information sought in this case is the content of the electronic communications of a Microsoft customer. The content to be seized is stored in Dublin . . . [I]t is our view that the invasion of the customer’s privacy takes place under the SCA where the customer’s protected content is accessed—here, where it is seized by Microsoft, acting as an agent of the government. Because the content subject to the Warrant is located in, and would be seized from, the Dublin datacenter, the conduct that falls within the focus of the SCA would occur outside the United States, regardless of the customer’s location and regardless of Microsoft’s home in the United States."

The court acknowledged the government's concerns that preventing SCA warrants from reaching data stored outside the US would seriously impede law enforcement and investigation efforts, especially given the government's view that the current process for obtaining non-US stored data, via Mutual Legal Assistance Treaties (MLATs), is "cumbersome" at best. These "practical considerations," however, could not overcome the text and history of the SCA, all of which led the court "to conclude that an SCA warrant may reach only data stored within United States boundaries."

The court was equally unpersuaded by the government's efforts to import the law developed in the subpoena context into the SCA's warrant provisions. Per the court, Microsoft "convincingly observe[d]" that the court has never approved the use of a subpoena to compel a recipient "to produce an item under its control and located overseas when the recipient is merely a caretaker for another individual or entity and that individual, not the subpoena recipient, has a protectable privacy interest in the item." Moreover, the court noted that, pursuant to the SCA's requirements for the type of data at issue, the government obtained a warrant, not a subpoena, rendering it inappropriate to analyze the dispute on the basis of the government's (broader) subpoena power.

In its conclusion, the court reiterated that "the SCA does not authorize a U.S. court to issue and enforce an SCA warrant against a United States-based service provider for the contents of a customer's electronic communications stored on servers located outside the United States. The SCA warrant in this case may not lawfully be used to compel Microsoft to produce to the government the contents of a customer's e-mail account stored exclusively in Ireland."

IMPLICATIONS

The Second Circuit's decision is a significant victory for Microsoft and other US technology companies that have been increasingly active in challenging the government's efforts to obtain confidential customer data, especially when the production of such data would raise privacy issues in jurisdictions outside the United States whose laws may restrict such disclosures. The ruling is also a blow to the government's expansive reading of its authorities under the SCA, though it may help ease the concerns of privacy advocates and regulators, especially in Europe, regarding the reach of US law into e-mail communications.

The Second Circuit's decision is unlikely to be the last word on the issue. The government can seek rehearing in the appellate court, and can seek leave to appeal to the US Supreme Court. The decision itself is binding only within New York and the other states within the Second Circuit, and the government can be expected to litigate these issues aggressively in other federal courts. If those courts reach different conclusions concerning the application of the SCA to cloud data located outside the US, it is likely that the issue will ultimately be settled by the US Supreme Court. The decision may also add pressure on Congress to update the terms of the SCA to better align the legal framework with 21st century technological realities.

LEGAL NOTICE

The contents of this publication are for reference purposes only and may not be current as at the date of accessing this publication. They do not constitute legal advice and should not be relied upon as such. Specific legal advice about your specific circumstances should always be sought separately before taking any action based on this publication.
