The CLOUD Act's Remedy for Microsoft-Ireland Has One Glaring Omission

MARCH 13, 2018

Robyn Greene
Policy Counsel and Government Affairs Lead, New America's Open Technology Institute

The Clarifying Lawful Use of Overseas Data Act (CLOUD Act, S. 2383, H.R. 4943) was recently introduced in the Senate and the House of Representatives. This bill is intended to accomplish two goals: First, it would allow qualifying foreign governments to bypass the Mutual Legal Assistance Treaty (MLAT) process when seeking data in criminal investigations and instead seek data directly from U.S. technology companies. As we describe in a separate in-depth analysis, this proposal lacks necessary safeguards and would threaten the privacy and human rights of Americans and internet users around the world.

Second, the CLOUD Act would change the law to enable the U.S. government to compel U.S. providers to hand over users' data even if those data are held outside the United States. The Supreme Court recently heard oral arguments in the Microsoft-Ireland case, where Microsoft, supported by amici curiae, including New America's Open Technology Institute, is challenging a warrant issued by a U.S. court under the Stored Communications Act (SCA) for data that are stored in Ireland. Microsoft argues that this would constitute an impermissible extraterritorial application of the SCA. The CLOUD Act would resolve this question in favor of the government, by explicitly providing that orders under the SCA would apply to the content of communications regardless of whether the information "is located within or outside of the United States." However, in so doing, the bill would raise a critical concern: it would fail to close the loophole that allows the government to warrantlessly access communications contents that are over 180 days old.

Current Law Governing the Contents of Communications Held By U.S. Providers

The SCA governs when electronic communications and remote computing service providers can hand over the contents of their users' communications. To obtain the contents of any communication that is under 180 days old, the government must get a warrant based on probable cause (18 U.S.C. 2703(a)).

The law does not state that the government can enforce a warrant issued under the SCA extraterritorially. Rules of statutory construction (legal canon) and Supreme Court precedent provide that unless Congress has specified otherwise, federal statutes are applicable and enforceable only in the United States or its territories; thus, search warrants do not have extraterritorial reach.

In the Microsoft-Ireland case, argued in the Supreme Court on February 27th, Microsoft refused to hand over the data, arguing that the warrant did not have extraterritorial effect and that the U.S. government would have to follow Irish legal process to obtain them. While the U.S. government agrees that the SCA cannot be applied extraterritorially, it contends that because the data would be handed over in the U.S., the warrant would not be applied extraterritorially, and it is therefore enforceable. The Court now has to determine whether, by forcing Microsoft to reach into Ireland to obtain the data, it would be enforcing the warrant extraterritorially, which would be unlawful.

As the Court is considering this case, Congress has been debating various legislative solutions. The CLOUD Act, which draws upon the International Communications Privacy Act (ICPA, S. 1671) is the most recent legislative proposal to seek to update the statute to ensure that U.S. law enforcement can reach communications content even when a U.S. company stores data abroad.

For more information, contact Robyn Greene, Policy Counsel and Government Affairs Lead, New America's Open Technology Institute, at greene@opentechinstitute.org.

The CLOUD Act's Microsoft Remedy: U.S. Law Governs, Pursuant to a Comity Analysis

The CLOUD Act would resolve the issue raised in the Microsoft Ireland case in favor of the government's position. If a U.S. provider receives legal process under 18 U.S.C. 2703 for the contents of a user's communications, it would have to disclose them to the U.S. government irrespective of where the data are located. However, the CLOUD Act would provide that a company in receipt of such a demand could file a motion to quash or modify it within 14 days of its receipt, if the company believed the order was inconsistent with the laws of another qualifying country. That motion would have to show that the company reasonably believes "(i) that the customer or subscriber is not a United States person and does not reside in the United States; and (ii) that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government" (Sec. 3(b) "§2713(h)(2)(A)").[1] While the motion is pending, the company would be required to preserve the subject data, but it would not be required to hand them over to the government, unless the court finds that immediate production is necessary (Sec. 3(b) "§2713(h)(4)).

The CLOUD Act would resolve the issue raised in the Microsoft Ireland case in favor of the government's position.

Upon receiving the motion, the court would have to determine whether to modify or quash the order pursuant to a comity analysis as specified in the CLOUD Act. In order to modify or quash the legal process, the court would be required to find that the company would violate the laws of a qualifying foreign government if it responded to the required disclosure and that the demand pertains to a non-U.S. person who does not reside inside the U.S. (Sec. 3(b) "§2713(h)(2)(B)(i and iii)"). The court would also have to make a determination that "based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed" (Sec. 3(b) "§2713(h)(2)(B)(ii)").

The bill sets forth the comity analysis that the court must undertake to determine whether the "totality of the circumstances" test has been met. That analysis prescribes that judges consider, as appropriate, a number of factors to determine if justice will be best served by enforcing the demand, or by modifying or quashing it. Those factors include the interests that the U.S. government has in obtaining the data; the interests the qualifying foreign government has in preventing their disclosure; the "likelihood, extent, and nature of penalties to the provider or any employees" as a result of the conflict of law; the location and nationality of the person whose communications are the subject of the demand, and the extent of their connection to the U.S., the extent of the company's connection to the U.S., how important the requested information is to the investigation, and whether the data could be obtained in a timely and effective manner through other means that would not incur negative consequences (Sec. 3(b) "§2713(h)(3)).

[1] A qualifying foreign government is a government with which the U.S. government has entered into a bilateral agreement enabling the governments to bypass the MLAT process and request data directly from electronic and remote computing service providers. To enter into one of these agreements, the Attorney General, in concurrence with the Secretary of State, must certify to Congress that the foreign government meets certain requirements related to human rights.
The process for entering into bilateral agreements that enable the MLAT process to be bypassed, and for the executive branch determination as to which countries may be a party to these bilateral agreements, is laid out in the second half of the CLOUD Act. OTI strongly opposes this process because it fails to provide adequate safeguards for privacy and human rights. An in-depth analysis of the CLOUD Act's proposed MLAT bypass process is available here: https://na-production.s3.amazonaws.com/documents/Cloud_Act.pdf.

Fatal Flaw: Failure to Mandate a Warrant-for-Content Causes Problems for the Microsoft-Ireland Remedy

While the comity analysis in the CLOUD Act provides courts with a way to adjudicate questions about conflicts of laws, this part of the bill still lacks an essential privacy protection. Unlike with previous iterations, such as ICPA, the CLOUD Act does not include a warrant-for-content fix that would close the 180-day loophole.

The CLOUD Act's failure to include a warrant-for-content fix is particularly troubling because it would mean that the U.S. government still would not be required to obtain a warrant before demanding contents from U.S. providers if the communication is over 180 days old.

As mentioned above, the warrant requirement in the SCA only applies when the government is seeking the contents of communications that were created within 180 days of the request (18 USC 2703(a)). If a communication is 181 days old, the law would require that a company hand over its contents pursuant to a 2703(d) order, which does not require a showing of probable cause of a crime (18 USC 2703(d)).[2]

It has been over 30 years since the Stored Communications Act became law. At the time it passed, data storage was exorbitantly expensive, so imposing a 180-day limit may have seemed reasonable at the time. Today, however, we are able to store hundreds of gigabytes of data for pennies - sometimes even for free - so individuals commonly save their communications well in excess of 180 days. Years of advocacy to close this loophole have resulted in two unanimous votes in the House of Representatives, but neither of those bills have received votes in the Senate. The result is a law that has not kept pace with technology and that does not appropriately apply the requirements of the 4th Amendment to the digital age.

The CLOUD Act's failure to include a warrant-for-content fix is particularly troubling because it would mean that the U.S. government still would not be required to obtain a warrant before demanding contents from U.S. providers if the communication is over 180 days old. As a matter of practice, the Department of Justice's (DOJ) current policy is to obtain a warrant for those communications, due to the Warshak decision by the U.S. Court of Appeals for the Sixth Circuit, which held that a warrant is constitutionally required to obtain email content.[3] The codification of the CLOUD Act's new rule that SCA orders served on U.S. providers are effective regardless of whether the data are stored abroad could result in DOJ abandoning this policy in investigations targeting the communications of non-U.S. persons who are located abroad.

The CLOUD Act's Microsoft-Ireland remedy should be amended to once-and-for-all close the SCA's 180-day loophole and require a warrant for all contents.

---

2 Orders under 18 USC 2703(d) can be used to obtain the contents of communications that are over 180 days old, and sensitive types of metadata, such as web browsing history. To obtain a 2703(d) order, the government must offer the court "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."

3 In United States v. Warshak (2010), the U.S. Court of Appeals for the Sixth Circuit ruled that the 180-day limit on the warrant requirement in the Stored Communications Act is unconstitutional. In response, many companies have started to refuse to hand over the contents of their users' communications unless the government obtains a warrant. However, this ruling is only precedential in the Sixth Circuit. As such, unless Congress acts to close the 180-day loophole, a different Circuit could compel a company to hand over data without a warrant, or a company could chose to had over data without a warrant.