Legal Sidebar

Email Privacy: District Court Rules that ECPA Warrants Apply to Electronic Communications Stored Overseas

3/4/2015

A pending case in the U.S. Court of Appeals for the Second Circuit could have important implications for the privacy protection afforded emails stored overseas. The case concerns the Electronic Communications Privacy Act (ECPA), the primary federal law governing private and government access to stored electronic communications.

Section 2703(b) of ECPA permits the government to obtain a subpoena or court order requiring an Internet Service Provider (ISP) to disclose the contents of electronic communications if the communication has been stored for longer than 180 days, or if it is being "held or maintained" "solely for the purpose of providing storage or computer processing services." Applicants seeking such an order must provide "specific and articulable facts, showing that there are reasonable grounds to believe that the contents of a[n] ... electronic communication ... are relevant and material to an ongoing criminal investigation." Alternatively, if the government seeks access to the content of an electronic communication that has been in "electronic storage" for 180 days or less, pursuant to section 2703(a) of ECPA, it must seek a warrant based on probable cause. The statute also provides that the government may use greater process when less would be sufficient – in other words, the government may choose to seek a warrant based on probable cause when only a subpoena based on reasonableness is required.

In the case, the United States sought and received a warrant from a federal magistrate judge under 2703(a) for the contents of emails and subscriber information for an email account operated by Microsoft Corporation. Microsoft complied with the portion of the warrant seeking non-content information, which was stored on servers located inside the United States. However, Microsoft determined that the content information sought by the warrant was located in servers hosted in Dublin, Ireland and moved to quash that aspect of the warrant.

In challenging the legality of the warrant, Microsoft argued that because federal courts lack authority to issue warrants for the search and seizure of items located outside of the United States, the warrant issued here was therefore unauthorized. The court rejected this argument, ruling that it was "undermined" by the structure of the governing statute, the statute's legislative history, and the practical consequences of adopting such reasoning. The court explained that the principles of extraterritoriality – which, among other things, limit a federal court from issuing a warrant for items overseas – were not implicated by warrants issued under ECPA. Section 2703(a) warrants were not traditional warrants but hybrids, with aspects similar to both subpoenas and traditional warrants. Like traditional warrants, the government applies to a neutral magistrate and must show probable cause; but like subpoenas, the order is served on the ISP that produces the information itself, rather than via a search by government agents. In contrast to traditional warrants, subpoenas require the disclosure of information within a recipient's control, regardless of location (even if overseas). In addition, when executing 2703(a) warrants, government officials do not view any information until it arrives in the United States, so no extraterritorial search occurs.

Turning to the legislative history, the court noted that Congress appeared to have expected that ISPs served with 2703(a) warrants would have to produce information within their control, regardless of where it is stored. The court observed that language in a committee report accompanying the Patriot Act – which partially amended section 2703(a) by permitting federal courts with "jurisdiction over the offense" to issue warrants – indicated that property was located with the ISP itself, rather than the location of a specific

server.

Similarly, the practical implications of applying the territorial limitations of traditional warrants to 2703(a) warrants indicated that Congress did not intend to restrict them to information stored in the U.S. Because ISPs often assign the storage of account information to a server located near an individual's claimed residence, and there is no obligation to be truthful in providing this information, a party seeking to avoid the reach of a 2703(a) warrant may simply claim a residence located overseas. In addition, conventional search warrants may only be executed overseas pursuant to a Mutual Legal Assistance Treaty (MLAT) – a treaty voluntarily executed between two countries – and the United States does not have such agreements with every country. Even when one is in place, executing a search warrant is a somewhat "laborious" process that generally permits one nation to decline a request.

Finally, the court noted that the concerns animating the principle of extraterritoriality – which teaches that when a statute gives no clear indication of application overseas, it has none – were inapplicable here. The execution of 2703(a) warrants does not criminalize conduct that takes place overseas; it does not require the deployment of law enforcement officers in a foreign country; and does not even require conduct of ISP employees overseas. Instead, at least in this situation, it only obligates the ISP to take action within the United States.

The magistrate judge thus denied the motion and upheld the warrant, and the district court affirmed. The case has been appealed to the Second Circuit Court of Appeals, and a variety of parties have filed amicus briefs with the court, perhaps reflecting the potential implications of the case for corporations and privacy protection.

Posted at 03/04/2015 01:33 PM by Jared P. Cole | Share Sidebar

Category: Privacy, Cybersecurity