It's Time For A Change In US Digital Privacy Laws


Samuel Miller

It is the rare legal issue where the ACLU, the National Association of Manufacturers and the U.S. Chamber of Commerce end up on the same side. But that is currently the situation in a case pending before the federal court of appeals in New York, where these entities and other major corporations have lined up in support of Microsoft Corporation.

Microsoft is challenging a lower court order requiring it to turn over all of the email communications of a subscriber to federal law enforcement officials pursuant to a search warrant, even though the email communications are stored on a Microsoft server in Ireland and the general rule is that a warrant has no effect outside of the territorial limits of the U.S. Thus, the pending case raises important constitutional issues regarding the power of government officials to seize private email communications pursuant to a warrant where the emails are stored overseas, the privacy rights of the email subscriber, the potential conflict between U.S. law and the privacy laws of Ireland and the European Union, and the potential conflict between law enforcement needs and personal privacy. The case is further complicated because the court will be forced to interpret an outdated electronic privacy law that was passed in 1986, when modern cloud computing and infinite digital storage were never contemplated.

The Outdated Federal Law Governing Access to Electronic Communications

The basic federal law governing protection and access to electronic communications is the Electronic Communications Privacy Act of 1986. The passage of this law was intended to protect the privacy of electronic communications, while balancing the legitimate needs of law enforcement to access records stored by the companies which enabled email communications or stored such communications. Given the technological capabilities at the time, it was assumed by Congress that email service providers would write over or destroy emails after more than 180 days. It was also assumed that the recipient would store an opened email on his or her own computer, and that an opened email would not be maintained by the email service provider. Thus, in terms of the procedures set forth in the ECPA to be used by law enforcement officials to request information from email service providers, the law contains distinctions which make little sense today: between emails more or less than 180 days old; between opened and unopened emails; between providers of "electronic communication service" and "remote computing service"; and between what electronically-stored information may be obtained by a subpoena as opposed to a search warrant.

The question of whether a search warrant is required for the government to obtain access to email communications raises constitutional concerns. The Fourth Amendment prohibits law enforcement officials from engaging in "unreasonable searches and seizures" of "persons, houses, papers, and effects." The Fourth Amendment further stipulates that a search warrant may only be issued by a neutral judicial officer after law enforcement presents a sworn statement establishing "probable cause" that a crime has been committed and "particularly describing the place to be searched, and the persons or things to be seized."

Thus, a search warrant is only issued by a neutral judicial officer upon a showing a "probable cause." In contrast, government law enforcement officials can issue subpoenas without approval of a neutral judicial officer and without a showing of "probable cause". Further, it is well-established that U.S.

courts are not empowered to issue search warrants — at least for the seizure of physical objects — outside of the U.S.

The current language of the ECPA only requires warrants for emails stored for less than 180 days, not for all emails, and can be served on the email service provider requiring it to turn over all the contents of an email account without notice to the subscriber. The law does not explicitly specify whether a warrant issued under the ECPA reaches email contents stored outside of the U. S., although the government asserts that an ECPA warrant requires a U.S.-based cloud or email service provider to access, copy and turn over emails stored overseas — conduct that all supposedly takes place in the United States.

Recent Technological and Judicial Developments Support Revisions to the ECPA

The ecosystem supporting electronic communications has changed dramatically since 1986. Then storage capacity was limited, and the prevalent computing model called for most information to be stored on individual personal computers. Today, vast amounts of personal and business information are stored in the "cloud," which is accessed remotely from anywhere in the world. Moreover, cloud computing companies and electronic communications service providers store information throughout the world. And storage capacity is so vast that emails, photos and other attachments are stored forever. These technological advances have Fourth Amendment implications.

Recent judicial decisions have expanded Fourth Amendment protections to digital files, based on the recognition that so much private information is now stored digitally. The U.S. Supreme Court ruled in the 2014 case of Riley v. California that a search warrant is generally required before police can search the contents of cellphone, even if on the person of someone who is lawfully arrested, because a cellphone may contain "every piece of mail [a person] has received for the past several months, every picture they have taken, or every book or article they have read."

Clearly, an email account, like a cellphone, can contain "a digital record of nearly every aspect of [a person's] life — from the mundane to the intimate." Because of this, a federal appellate court has expressly held in U.S. v. Warshak that the seizure of private emails by the government requires a search warrant. The court ruled that, just as a sealed letter cannot be opened by government law enforcement without a warrant, government agents cannot require an email service provider to turn over the contents of a subscriber's email account without obtaining a search warrant, unless a specific exception to the warrant requirement applies.

Finally, in a 2010 decision, the Supreme Court confirmed that federal laws should not be presumed to apply outside of the U.S. unless Congress clearly says so. But these recent technological and judicial developments are not reflected in the outdated language of the ECPA.

The Feds vs. Microsoft

Federal law enforcement officials applied for a search warrant under the ECPA, and the U.S. magistrate issued the warrant, authorizing the seizure of all the contents of an email account of a Microsoft email subscriber. Microsoft complied with the search warrant by providing the government with information about the account and the subscriber to the extent that such information was stored in the U.S. However, Microsoft challenged the warrant to the extent that it required Microsoft to copy and turn over to the government the contents of all email communications, which were stored in a server located in Ireland, and operated by Microsoft's Irish subsidiary.

The government sought enforcement of the warrant. The lower federal court ordered Microsoft to comply and held Microsoft in contempt for refusing to comply. The lower federal court interpreted the ECPA to require Microsoft to respond fully to a warrant by producing information within its control, and accessible in the U.S., regardless of where that information is stored. The lower court rejected Microsoft's argument that federal courts are without authority to issue or enforce warrants for the search and seizure of property, including the contents of an email account, stored in another country. The court interpreted the ECPA to compel Microsoft to copy and turn over the email contents stored in Ireland, reasoning that law enforcement efforts could be seriously impeded if the territorial restrictions on conventional warrants applied to warrants issued under the ECPA. These are the legal rulings which Microsoft has challenged in the Second Circuit Court of Appeals.

Criticisms of the Lower Court Ruling

As AT&T succinctly argued in support of Microsoft in the court of appeals:

> The district's court's overbroad construction of the [ECPA] is bad for American foreign relations (because it intrudes on the sovereignty of U.S. trading partners), bad for American business (because it threatens relationships with foreign consumers), bad for American citizens (because it invites reciprocal intrusions into U.S.-located data from foreign states that do not have any legitimate regulatory interest in the data and that may have far less protective data protection regimes) and bad for the future of the Internet, digital technology and consumer applications (because it invites countries to wall off and segment information so that it cannot be reached by U.S. law enforcement).

The Republic of Ireland also weighed in before the appellate court, pointing out that the lower court order is an intrusion on Ireland's sovereignty and that federal officials should have proceeded by requesting Irish law enforcement to obtain the requested information through an existing Mutual Legal Assistance Treaty between Ireland and the U.S.

Congress Should Update the ECPA

Rather than wait for courts to struggle interpreting an outdated law, it would make more sense for Congress to pass an updated and modernized digital privacy law.

Last fall, an effort to do this was undertaken by U.S. Senators Orrin Hatch, R. Utah, Chris Coons, D. Del., and Dean Heller, R. Nev., who introduced the Law Enforcement Access to Data Stored Abroad Act ("LEADS Act"). Although this act died in committee last year, it was reintroduced on Feb. 12, 2015. This proposed legislation abolished the outdated 180-day distinction and updated the ECPA to require a warrant to search any email content, in line with the Warshak decision.

The proposed legislation further clarified the ECPA to authorize the government to use a warrant served pursuant to the ECPA to obtain email content of U.S. persons regardless of where the email content was stored. However, the proposed legislation made clear that the ECPA should not authorize warrants to obtain content of a non-U.S. person stored outside the U.S., because enforcing such a warrant may infringe the sovereignty of the subscriber's home nation.

With respect to requests for the email content of foreign subscribers stored in other countries, the LEADS Act directs federal authorities to utilize mutual legal assistance treaties or other similar arrangements in cooperation with foreign governments. Addressing the trends in some countries, especially in the EU, that requires data generated in the EU to be stored in the EU, the act expressed the sense of Congress that such data localization requirements imposed by foreign governments on data providers are incompatible with the borderless nature of the Internet and would be an impediment to online innovation.

In explaining why he supported the bill, Sen. Coons said in a statement that, "law enforcement agencies wishing to access Americans' data in the cloud ought to get a warrant, and just like warrants for physical evidence, warrants for content under ECPA shouldn't authorize seizure of communications that are located in a foreign country. The government's position that ECPA warrants do apply abroad puts U.S. cloud providers in the position of having to break the privacy laws of foreign countries in which they do business in order to comply with U.S. law. This not only hurts our businesses' competitiveness and costs American jobs, but it also invites reciprocal treatment by our international trading partners."

Imagine the outcry if Chinese officials served an order in China on a subsidiary of a U.S.-based email or cloud service provider demanding that all the emails of a Chinese dissident stored in the U.S. be turned over to the Chinese authorities, even if the Chinese dissident now lived in the U.S. Yet the lower court ruling allows the U.S. government to make such a demand.

Updating and modernizing the ECPA is a bipartisan issue that deserves congressional action.

Indeed, just recently, bipartisan bills amending the ECPA were introduced by a number of senators

and congressmen. See H.R. 283 and S. 356 (114th Congress). While this new proposed legislation is positive, it does not address the extraterritorial reach of an ECPA warrant. As Sen. Hatch stated in reintroducing the LEADS bill:

> While I agree in principle with the ECPA reform bills recently introduced into the House and Senate, neither establishes a framework for how the U.S. government can access data stored abroad. As Congress works to reform our domestic privacy laws, we must modernize the legal framework for government access to digital data stored around the world. This bill recognizes that these two issues are inextricably linked.

Thus, as Congress considers the proposed Electronic Communication Privacy Act Amendments Act of 2015 and the newly reintroduced LEADS act, it might add provisions consistent with the following principles:

First, digital content in a person's or company's email or cloud-computing account is owned by that individual or company, and should not be considered a business record of the cloud-computing or email communication provider.

Second, in order to obtain such digital content, law enforcement officials should proceed by obtaining a search warrant, supported by "probable cause."

Third, a court should only approve an application for an ECPA warrant if the government establishes a "substantial nexus" between the U.S. and the information sought. This can be established if the data is stored in the U. S.; or if the data at issue belongs to a U.S. citizen or resident; or if the content was generated pursuant to a U.S.-based service or transaction; or when the government can satisfy the court that there is some other substantial connection between the information sought and the U. S., beyond the mere fact that the parent entity of the email or cloud provider is U.S.-based. If such a "substantial nexus" cannot be established, then the district court could refuse to issue the warrant and require law enforcement to seek foreign-based information through mutual legal assistance treaties or other procedures, such as a subpoena with notice to the subscriber and the country where the data is located.

Such principles would be consistent with Congress' presumed intent to regulate only domestic matters, while respecting the sovereignty and data privacy laws of other countries. Such principles also strike an appropriate balance between law enforcement needs and privacy rights.

—By Samuel R. Miller