The Media Institute

Policy Views

UPDATING THE ELECTRONIC COMMUNICATIONS PRIVACY ACT: AN ESSENTIAL LEGISLATIVE GOAL FOR MEDIA COMPANIES AND THE PUBLIC THEY SERVE

Kurt Wimmer

I. The Need for Reform: A 1986 Act Doesn't Fit the 2015 Cloud

One of the most important technological innovations of the past decade has been the emergence of "cloud computing." In essence, cloud computing refers to the ability of computer users to process and store their data remotely – at an off-site datacenter – rather than on a local machine. When content is stored "in the cloud," it can be accessed from any computer with an Internet connection, which makes it more easily shared, edited, and published.

Individual computer users have been familiar with one form of cloud computing – Web-based e-mail (*e.g.,* Hotmail, Gmail) – since the late 1990s. In the past five to seven years, cloud computing has been increasingly embraced by a range of institutional entities, including corporations, nonprofits, and governmental entities. Cloud computing also has revolutionized the news industry. The cloud enables reporters working on all platforms – digital, television, and print – to use new tools to gather multimedia content, and it also allows their news organizations to deliver that content efficiently to consumers.

In an era of tight budgets for newsrooms and infrastructure, cloud computing has helped many media companies reduce costs and make their newsgathering operations more efficient and effective. It can be much more efficient for a newsgathering and

publishing operation to purchase a package of cloud-based services (*e.g.,* word processing, photography, publishing, storage) rather than maintain its own IT department, servers, and software.

Although there are substantial advantages for media companies in adopting cloud-based technologies, there also are risks. Newsgathering operations routinely handle highly sensitive information, and they rely on a foundation of trust between reporters and their confidential sources. If a media organization concludes that entrusting its data with a cloud service provider will result in that data being less private or secure, then the organization is less likely to embrace cloud technologies. This concern is not mere speculation; the government repeatedly has undertaken surveillance on journalists in recent years. For instance, in 2013, the public was shocked to learn that the Justice Department had secretly monitored Fox News reporter James Rosen's personal e-mail and cell phone records as part of an investigation into an alleged leak of classified information. Also that year, the public learned that the Justice Department secretly used a subpoena to obtain phone records of more than 20 phone extensions at the Associated Press covering scores of journalists' work. These revelations came as the Fourth Circuit – home jurisdiction for many government defense and intelligence agencies – ruled that the First Amendment does not shield journalists from being compelled to reveal their sources in criminal cases.

This concern has been accentuated by the controversy surrounding Edward Snowden's disclosures in 2013 regarding government surveillance. Particularly for media organizations with headquarters or operations outside the United States, the Snowden disclosures increased concern that if the companies entrusted their data to a U.S. cloud provider, that would make it easier for U.S. law enforcement to obtain their data.

Our increasing reliance on cloud storage and the Snowden disclosures thus have underscored the importance of clarifying the rules through which law enforcement can obtain customer content from cloud service providers. Additional clarity is urgently needed because the current law governing law enforcement access – the Electronic Communications Privacy Act ("ECPA") – was enacted in 1986, before the cloud truly existed. ECPA is accordingly outdated in important respects. For example, under

ECPA, 18 U.S.C. § 2703(a), the government can obtain e-mails stored for *180 days or less* only with a warrant. E-mails stored for *more than 180 days*, on the other hand, can be obtained with a simple subpoena – a form of legal process that does not require court pre-approval and can be issued upon less-than-probable cause. Whatever logic this distinction may have had in 1986, when e-mails and electronic documents might be considered abandoned if they had not been downloaded to local storage within six months, it is no longer rational in light of modern technological realities under which cloud storage is routinely used for long-term storage of confidential data. Our current storage habits for digital records are precisely the opposite of the habits that existed in 1986, when ECPA was adopted.

As technology has advanced – and as ECPA has become increasingly obsolete – courts have started to fill this gap by applying Fourth Amendment constitutional protections to data stored in the cloud. In an important 2010 decision, *United States v. Warshak*, the U.S. Court of Appeals for the Sixth Circuit held that users have a reasonable expectation of privacy in *all* of their e-mails – irrespective of how long they have been stored – and that the government may only obtain e-mails from cloud providers with a warrant issued on probable cause. But this approach is not uniform throughout the United States, leading to irrational results and inconsistent protections among residents of different judicial circuits.

Another respect in which ECPA has not kept pace with technology is the issue of extraterritoriality. ECPA does not on its face make clear how its rules apply to data stored outside the United States. This is not surprising, because in 1986 Congress did not consider the possibility that cloud providers might store customer data outside the United States. Since then, however, as cloud services have become increasingly globalized, providers have begun to store more of their data outside the United States and closer to their international customer base.

Under a long-standing legal principle – the "presumption against extraterritoriality" – a law does not apply outside the United States unless Congress clearly states that it was intended to have extraterritorial effect. Given ECPA's silence, it could rationally be assumed that ECPA would have no extraterritorial effect and would apply solely to data stored domestically. Microsoft has objected to a domestic request

for a customer's data under ECPA – relying on this presumption against extraterritoriality – to confirm that ECPA does not apply to customer content stored outside the United States. Microsoft has also argued that limiting ECPA to the territory of the United States prevents unnecessary conflicts with foreign data-privacy laws and avoids putting providers in the Catch-22 situation where they risk violating foreign law if they *do* produce customer data and risk violating U.S. law if they *don't*. The government has contested Microsoft's argument, and this case is currently being considered by the U.S. Court of Appeals for the Second Circuit in New York.

However the court rules in this particular case, it is clear that Congress has a role to play in updating ECPA for the era of cloud computing. As discussed in the following section, the bipartisan, bicameral LEADS Act introduced in the Senate on Feb. 12, 2015, by Senators Orrin Hatch (R-Utah), Chris Coons (D-Del.), and Dean Heller (R-Nev.), and in the House on Feb. 27, 2015, by Representatives Tom Marino (R-Pa.) and Suzan DelBene (D-Wash.), is an important step forward in this regard.

II. The Solution: The LEADS Act

The LEADS Act would update ECPA in two important respects. First, it would implement the principles of the *Warshak* decision on a nationwide basis by requiring law enforcement to obtain a warrant under ECPA to obtain the consent of *any* customer communications that are stored in the cloud. This would eliminate the outdated 180-day distinction currently in the law that affords older e-mails less protection than newer ones.

Second, it would create a comprehensive framework to address data stored outside the United States. In summary, the statute:

- ***Recognizes that, as a general principle, warrants issued under ECPA lack extraterritorial effect***. The starting point of the LEADS Act is a recognition that law enforcement may not use warrants to compel cloud providers to disclose customer content stored outside the United States. For such information, law enforcement should instead rely on Mutual Legal Assistance Treaties ("MLATs"), treaties designed and implemented for the express purpose

of allowing the government of one country to obtain evidence stored in a different country that is relevant to an ongoing criminal investigation.

- ***Addresses the reasonable requirements of law enforcement, by authorizing extraterritorial warrants for U.S. persons***. The LEADS Act takes account of the legitimate needs of law enforcement by permitting the government to obtain warrants for content if the account holder is a *United States person*, regardless of where that content may be stored.
- ***At the same time, the LEADS Act does not contravene the privacy laws of foreign countries.*** If a cloud service provider receives a warrant for the content of a U.S. person that is stored abroad – and if the data privacy law of the foreign country where the data is stored would bar disclosure of the data – then the provider can ask a U.S. court to vacate or modify the warrant.
- ***Strengthens the MLAT process***. The LEADS Act requires the attorney general to implement some common-sense reforms to make the MLAT process stronger and more streamlined. For example, the bill requires the government to create an online docketing system for MLAT requests, which allows foreign governments to track the status of MLAT requests filed by those governments.

In sum, the LEADS Act would create a comprehensive framework that would help address many issues presented by ECPA's increasing obsolescence. The legislation adds significantly to the ongoing legislative debate about modernizing ECPA. In particular, if the LEADS Act is enacted, then media companies will have greater clarity about the circumstances in which U.S. law enforcement can obtain their data – both stored inside and outside the United States. The bipartisan legislation has been introduced by key, senior members of both the Senate and House Judiciary committees, which indicates it will likely receive serious consideration this Congress.

From the perspective of the media, the LEADS Act is long overdue. Concerns about the security of confidential-source information that may be stored in the cloud, particularly on an international basis, may be holding back the media's use of the most efficient and effective technologies. Clarifying that the data in the cloud can be as secure

as data held on local servers would permit media companies, and the economy as a whole, to rely on cloud-based technologies that exist today, and that will be developed in the future. This issue and this Act are bi-partisan, common-sense, and workable solutions that Congress should embrace and pass as soon as possible.

Kurt Wimmer is the U.S. Chair of the Privacy and Data Security practice of Covington & Burling LLP and a partner in its Washington office. He is a member of the Board of Trustees of The Media Institute and chairs its First Amendment Advisory Council. Although he represents clients in the media and technology space, the opinions expressed in this paper are solely his own.

Policy Views are published by The Media Institute, a nonprofit research organization specializing in the First Amendment and communications policy. These papers are intended to provide timely analyses of communications policy issues. For more information, contact The Media Institute or visit our website at www.mediainstitute.org.

March 2015

The Media Institute * 2300 Clarendon Blvd., Suite 602 * Arlington, VA 22201
703-243-5700 * E-mail: info@mediainstitute.org * www.mediainstitute.org