Institute For Policy Innovation IPI Ideas
Innovative Insights on Today's Policy Debates
NO. 67 September 2015

Securing Our Rights Through ECPA Reform

by Bartlett D. Cleland

> "*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*"
>
> **Fourth Amendment, U.S. Constitution**

If the Fourth Amendment to the Constitution of the United States were being drafted today, James Madison, and George Mason before him, would likely not have used the word "papers" to describe various types of personal communications.

Much has changed since then, but the idea communicated in the amendment is still as clear as ever: that the people and anything they own must be protected from unreasonable government searches and seizures. And while that fundamental tenant of a citizen's protection has been the subject of much legal and judicial wrangling over the years, there is little doubt that such a basic protection should extend into the electronic realm as well.

Nearly 30 years ago, in 1986, Congress passed the Electronic Communications Privacy Act, or ECPA. The intention was to extend the already-existing restrictions on government wiretapping of telephone calls to the transmission of electronic data by computers, and to add provisions to the law to restrict access to stored electronic communications. So, ECPA provides law enforcement guidelines when they need to access data, but the guidelines have a glaring problem.

What's the Problem?

Under the law, if stored "communications" are kept for more than 180 days, they are considered "abandoned," which has been interpreted to mean that the owner no longer has any expectation of privacy in what was stored. Therefore, law enforcement can access that data without a warrant—as opposed to data less than 180 days old, which still requires the government to obtain a search warrant to acquire the data. Now, many decades later and with computing power doubling 20 times over since then, the concept of "transmission of electronic data by computers" as conceived then bears almost no relation to technology and practices today.

In 1986, even the most primordial World Wide Web was still three or four years away. So-called mobile phones were larger than a Dustbuster, limited to allowing the user to make and receive calls. Mobility as we understand it today and mobile broadband were still decades off. To the extent that people retained personal information, it was typically on a 5 ¼ inch floppy disk that whirred away for what today would seem like an eternity to save the smallest amounts of data. In addition to being cumbersome, the storage of data was expensive. As a result, emails and other communications were not routinely stored, and even if some backup was available and used, data was rarely kept more than 180 days.

Today, the availability of cheap, massive data storage has completely flipped our practice: the bias now is to save data, lots of data, for a long time. And an increasing amount of personal data, most easily described as "communications," is being stored in "the cloud," which is the remote storage of data with multiple redundant systems to ensure that the data is not lost. So, rather than storing your pictures, financial information, or just backups of personal emails to your computer's hard drive, cloud computing enables the storage of that information on remote servers designed to store data securely for an extended time. Such technological developments and practices were not contemplated during the drafting or enactment of ECPA resulting in intellectually inconsistent law. Using email

as an example, an email in transit (even what "in transit" means in an age of data packets is a complex discussion) or stored on a home computer requires a warrant. An email opened, or an email unopened for more than 180 days, merely requires a subpoena. The difference? A subpoena is a court order for a person, or documents, to appear or be provided. A warrant provides law enforcement with the authority to search and seize property, as well as arrest a person. Practically speaking, a subpoena is much easier to obtain, since a warrant requires a probable cause standard and must be issued by a judge.

The Solution: Update ECPA

Clearly, ECPA needs to be updated to ensure that a warrant is obtained before stored electronic data is released. ECPA also needs to be made more adaptable to future changes in technology and practices, so that the law no longer assumes that data kept for more than 180 days has been abandoned by its owner. In fact, the whole notion of abandonment of such property is increasingly hard to define, and maybe largely elusive, as today some business models even encourage the posting and storing of all sorts of online communications whether messages, pictures, or other data, for the long term. Holding onto old emails (or pictures or medical information) indefinitely is no different than keeping written correspondence from years earlier, which the Fourth Amendment clearly protects.

Treating data stored electronically as less protected than analog data—that is, data stored in our homes or offices—exposes a clear discrimination against technology. The result amounts to a loophole in well-recognized protections of our privacy and personal security.

We should strive to be a nation of laws, not a nation of loopholes. The challenge is in applying clear but older—and in some cases antiquated—terminology to current issues. Electronic data is no different than data on paper; indeed, all you need is a scanner to turn a document on paper into electronic data. But that shouldn't change the document's legal status.

Based on Property Rights

The fundamental issue that undergirds the guarantee of our security in our personal effects is the protection of property rights. Property rights form the foundation of our freedom and of the free market—and they must be protected. To ignore the current state of ECPA is to ignore our Fourth Amendment rights.

Put another way, if the Fourth Amendment is to be a protection, and a cornerstone protection at that, our digital data must be recognized as our property, and our property rights must be protected. The danger of not doing so is clear: Markets simply don't work without property rights. Contracts, sales, licensing—none of it can happen if clear and enforceable property rights are not guaranteed. All business models, not just "new" business models, rest on property rights.

The fix here is fairly simple—require that: "Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." In other words, fix ECPA so that electronic data is treated no differently than analog data.

Good News/Bad News

The good news is that legislation to update ECPA has been introduced in both the U.S. House and Senate, with broad, bipartisan support. In the U.S. House, the Email Privacy Act currently has 292 cosponsors—more than enough to ensure passage.

The bad news is that Congress has shown little urgency in moving the legislation. This is inexcusable, because in this case, good policy IS good politics. A January 2015 poll by Vox Populi Polling for the Digital 4th Coalition found that more than 80 percent of voters polled supported updating ECPA to enhance privacy.

Conclusion

Can there be any good reason, any good motive, for an unrestrained executive branch of government to be reading our emails, prying into our personal effects or peeking at our data without a warrant? This is not a debate about whether materials can be searched, but rather how and with what safeguards for citizens. Without an update to ECPA our Constitutional protections are at risk when we operate electronically, our rights sacrificed to the convenience of government.

There are many good reasons for updating ECPA, such as enhancing the ability of U.S. companies to compete effectively in the cloud computing market, and so that law enforcement can always access electronic communications in all appropriate situations. But none of these are as critical, or as fundamental, as updating the law to protect our rights.

Bartlett D. Cleland is the Resident Scholar of Tax and Innovation Policy for the Institute for Policy Innovation.

Institute for Policy Innovation: 1320 Greenway Drive, Suite 820 Irving, TX 75038

www.ipi.org phone: 972-874-5139 email: ipi@ipi.org