E-mail Digital Privacy

Paul Rosenzweig

Should the contents of e-mail messages be protected from unwarranted law enforcement scrutiny to the same extent as physical letters sent through the mail? To ask the question makes the answer seems obvious. E-mail is today's postal service, and the personal contents of e-mail messages are as private to people as the letters sent through the U.S. Postal Service.

But even though that answer seems obvious, it is not what the law states. Today, some of the contents of e-mail (most notably the e-mails stored on a server, such as through Gmail) are not as well-protected. In order to read Americans' mail that is in transit with the Postal Service, the government generally needs a warrant issued by a neutral magistrate, and must have probable cause to believe that the search will provide evidence of a crime. To read the content of e-mail messages stored on a cloud server, the government does not need a warrant at all—it can view the content by issuing a subpoena to the cloud service provider. Unlike a warrant, a subpoena is not based on probable cause and it is not reviewed by a judge before it is issued. In practice, it is issued by a prosecutor, is unchecked by a judge, and can be based on most any ground.

The reason for this difference in treatment is more historical than malevolent. The law that protects e-mail communications—the Electronic Communications and Privacy Act (ECPA)—was written in 1986, when Gmail did not exist, when cloud servers were a dream of the future, and when nobody could imagine storing e-mail for any length of time because digital storage costs were so high.

As a result, under current law, as data moves from local storage to the cloud, the government argues that it does not need to ask the owner of the data for permission to see it. Instead, the government claims that it can go to the cloud provider, demand the data with a subpoena, and prohibit the data owner from being notified. This law needs to change: When government agents want Internet service providers and cloud providers to disclose sensitive data, they should have to obtain a warrant from a judge.

In addition, the current rules are absurdly complicated. There is one rule for "opened" e-mail, a different rule for unopened. There is also one rule for e-mail less than 181 days old, and a different rule for e-mail 181 days or older. Even large companies, with teams of lawyers and paralegals, find the complexity of the law a burden. Start-ups must spend time and money on lawyers that would be better spent finding new ways to innovate.

In short, technology has changed the way Americas live. Today most people store their e-mails in the cloud. But the law has not kept up. That is why Congress needs to modernize the law. In both the last Congress and this one, Senators and Representatives have introduced bipartisan bills to make the ECPA relevant for the 21st century.[108] In the last Congress, the bill never made it to the floor of either body. In the 114th Congress, both chambers should give the proposals plenary consideration.

ECPA reform must not be allowed to affect intelligence investigations and counterterrorism programs. The Foreign Intelligence Surveillance Act has its own set of rules for government access to e-mail and documents stored in the "cloud." ECPA reform legislation will not affect those rules in any way.

The time is ripe for change and the principle is clear—in the normal law enforcement context, police and FBI officers should have no more access to Americans' stored e-mail than they do to private letters stored in a trunk in the attic.[109]

Endnotes

108. The Law Enforcement Access to Data Stored Abroad (LEADS) Act, S. 2871, 113th Cong., 2nd Sess., http://www.gpo.gov/fdsys/pkg/BILLS-113s2871is/pdf/BILLS-113s2871is.pdf (accessed May 4, 2015); The Law Enforcement Access to Data Stored Abroad (LEADS) Act, S. 512, 114th Cong., 1st Sess., https://www.govtrack.us/congress/bills/114/s512/text (accessed May 4, 2015); The Law Enforcement Access to Data Stored Abroad (LEADS) Act, H.R. 1174, 114th Cong., 1st Sess., https://www.govtrack.us/congress/bills/114/hr1174/text (accessed May 4, 2015); Electronic Communications Privacy Act Amendments Act of 2013, S. 607, 113th Cong., 1st Sess., https://www.congress.gov/bill/113th-congress/senate-bill/607/text (accessed May 4, 2015); Email Privacy Act, H.R. 1852, 113th Cong., 1st Sess., https://www.congress.gov/bill/113th-congress/house-bill/1852/text (accessed May 4, 2015); and Email Privacy Act, H.R. 699, 114th Cong., 1st Sess., https://www.congress.gov/bill/114th-congress/house-bill/699/text (accessed May 4, 2015).
109. For more information, see Evan Bernick, "Protecting Americans' Privacy: Why the Electronic Communications Privacy Act Should Be Amended," Heritage Foundation *Legal Memorandum* No. 118, February 28, 2014, http://www.heritage.org/research/reports/2014/02/protecting-americans-privacy-why-the-electronic-communications-privacy-act-should-be-amended.