Shuttering of Lavabit and Silent Mail Illustrate Potential Effects of a CALEA II

by Joseph Lorenzo Hall [1]
August 14, 2013

With all the news during this "Summer of Snowden," it can be easy to forget some of the issues that many of us worried about before the unprecedented sunlight cast into the U.S. surveillance apparatus. One of these issues, updates to the Communications Assistance for Law Enforcement Act (CALEA) ("CALEA II"), has resurfaced. With CALEA II, the FBI is pushing to expand to Internet applications the technology mandates of the 1994 CALEA statute, which requires telecommunications companies to design their services to be wiretap-friendly. Last week, two providers of encrypted email service – Lavabit [2] and Silent Circle's Silent Mail [3] – announced that they were shutting down given the prospect of secret government demands for access. The news raises concerns that the government may be, in effect, achieving the goals of CALEA II without Congress' approval and, moreover, with a sledgehammer.

For the past several years, various law enforcement officials have been pressing for updates to CALEA in order to require a wide variety of online services to be wiretap-capable, a move that CDT has opposed. CDT and others have argued that CALEA II could slow or even block the development of innovative products providing secure communications to businesses and individuals. This past spring, technology experts issued a report on CALEA II [4], arguing that requiring backdoors into end-point software and devices would make these products vastly less secure.

Fast forward to last week: the secure email service Lavabit voluntarily shut down, without notice, based on an undisclosed judicial order that Lavabit founder Ladar Levison said put the privacy of Lavabit's encrypted email users at risk. "Unfortunately, what's become clear is that there's no protections in our current body of law to keep the government from compelling us to provide the information necessary to decrypt those communications in secret," Levison was quoted [5] as saying. A few hours after Lavabit announced its closure, Phil Zimmermann, the creator of the widely used PGP encryption and co-founder of Silent Circle, announced [6] that Silent Circle had decided to shut down its secure email product too, anticipating judicial demands in the future similar to the order Lavabit received.

Secure communications tools are the backbone of modern e-commerce and, increasingly, of a wide range of online interactions. However, Lavabit clearly felt that it had to choose between violating the integrity of its users' communications or ceasing operations. Likewise, Silent Circle pre-emptively shut its Silent Mail service down in anticipation of having to make a similar choice in the future when facing government demands.

The result goes far beyond what Congress provided for even in CALEA I. That statute has a provision explicitly intended to preserve the ability of service providers to offer unbreakable encryption. ("A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier *and the carrier possesses the information necessary to decrypt the communication.*" 47 USC 1002(b)(3) (emphasis added)) CALEA I also explicitly states that it does not authorize "any law enforcement agency or officer to prohibit the adoption of any … service, or feature by any provider of a wire or electronic communication service." Moreover, CALEA I allows, indeed encourages, companies to disclose the surveillance features they adopt by providing a safe harbor for compliance with "publicly available technical requirements or standards."

What did the government demand and under what authority prompted Lavabit's shutdown? We don't know, and that's part of the problem. The Wiretap Act, which authorizes the government to intercept communications content prospectively in criminal investigations, indicates that a provider of wire or electronic communication service (such as Lavabit) can be compelled to furnish law enforcement with "all information, facilities and technical assistance necessary to accomplish the

interception unobtrusively… .” 18 USC 2518(4). The Foreign Intelligence Surveillance Act (FISA), which regulates surveillance in intelligence investigations, likewise requires any person specified in a surveillance order to provide the same assistance (50 USC 1805(2)(B)) and so does the FISA Amendments Act with respect to directives for surveillance targeting people and entities reasonably believed to be abroad (50 USC 1881a(h)(1)). The “assistance” the government demands may include the disclosure of the password information necessary to decrypt the communications it seeks, *if* the service provider has that information, but modern encryption services can be designed so that the service provider does not hold the keys or passwords. Was the “assistance” that the government demanded of Lavabit a change in the very architecture of its secure email service? Was the “assistance” the installation of the government’s own malware to accomplish the same thing? Lavabit has not answered these questions outright, but it did make it clear that its concern extended to the privacy of the communications of all of its users, not just those of one user under one court order.

We think the law is clear: if you’ve built a secure email service, the government can’t secretly force you to break it and rebuild it to be insecure under the “provider assistance” mandate that might accompany a surveillance order or directive. If that's what the government is demanding here, then we have CALEA II design mandates imposed by secret court order, going far beyond anything that Congress ever intended with the “assistance” requirements of current law and far beyond anything in CALEA I.

If it is the government’s theory that existing law already empowers it to demand secret alterations in communications services, then the shutdowns of Lavabit and Silent Mail are very troubling indeed. Take just one concern: the personal safety of human rights activists who depend on secure email service in carrying out their work. The U.S. government has actually supported the development of secure communications tools for human rights activists. Does the shutdown of Lavabit mean that secure email services cannot be secure against government access? Or does it say the U.S. will not tolerate in the U.S. the kind of secure communications it is promoting in Iran or Tibet?

Last week, President Obama committed his Administration to being more forthcoming about its surveillance activities in order to engender public trust. Allowing Lavabit to explain what it was about the government’s surveillance demands that prompted the company to shut down its service would go a long way toward building that trust. It would also tell us whether we can trust any service that promises security online. A negative answer to that question would have profound implications for both commerce and the democratic potential of the Internet.

Links:
[1] https://cdt.org/personnel/joseph-lorenzo-hall
[2] http://lavabit.com/
[3] https://silentcircle.com/web/silent-mail/
[4] https://www.cdt.org/files/pdfs/CALEAII-techreport.pdf
[5] http://news.cnet.com/8301-1009_3-57597954-83/lavabit-chief-predicts-long-fight-with-feds-q-a/
[6] https://silentcircle.wordpress.com/2013/08/09/to-our-customers/