Lavabit email shuts down after refusing to comply with “crimes against the American people”

Steve James
10 August 2013

Texas-based secure email provider Lavabit has closed down its operations rather than “become complicit in crimes against the American people” by complying with demands from the US government, apparently for access to the mail company’s servers and customer information.

On Wednesday, Lavabit, which has about 350,000 users, posted a notice on its website from owner Ladar Levinson.

Levinson wrote. “I have been forced to make a difficult decision: to become complicit in crimes against the American people or walk away from nearly ten years of hard work by shutting down Lavabit.”

He explained that after “significant soul searching, I have decided to suspend operations. I wish that I could legally share with you the events that led to my decision. I cannot. I feel you deserve to know what's going on—the first amendment is supposed to guarantee me the freedom to speak out in situations like this. Unfortunately, Congress has passed laws that say otherwise. As things currently stand, I cannot share my experiences over the last six weeks, even though I have twice made the appropriate requests.”

Levinson warned that “without congressional action or a strong judicial precedent, I would strongly recommend against anyone trusting their private data to a company with physical ties to the United States.”

The persecution of Lavabit by the US government is undoubtedly connected to the fact that the company’s most well-known client is whistleblower Edward Snowden. It is also aimed at undermining the ability of internet users to easily engage in secure communication that cannot be accessed by the National Security Agency.

Two months ago Snowden, a former intelligence contractor at Booz Allen Hamilton, exposed the architecture of the unprecedented and all-pervasive internet surveillance regime operated by the US government’s NSA and its allies around the world. Snowden is the target of an unprecedented international manhunt orchestrated from the US. He has been given temporary asylum in Russia, although his security and life remain in great danger.

Snowden is reported to have been a Lavabit user since 2010. It is likely that Lavabit has, at the very least, received orders from the Foreign Intelligence Surveillance Court (FISA) seeking metadata and content from Snowden’s email history or similar request from the US surveillance agencies.

Those on the receiving end of FISA rulings are generally mandated to not reveal any information about what they have been asked to turn over. Should those under investigation become aware of the efforts directed against them, the government can issue a gag order insisting that nothing is made public.

Lavabit's action is likely in response to government demands that go beyond Snowden. According to the *Wired* website, court records show that in June Lavabit complied with a “routine search warrant targeting a child pornography suspect in a federal case in Maryland... Whatever compelled him [Levinson] to shut down now must have been exceptional.”

Lavabit may have received demands for the sort of blanket access to its services that, according to Snowden’s exposures, has been given to the NSA by Google, Yahoo, Microsoft, Facebook and a swathe of major US tech corporations under their PRISM and related spying programs.

© World Socialist Web Site

Lavabit's encrypted email provision was viewed as among the most secure in the world. The company was founded in 2004 as Nerdshack LLC, specifically in response to concerns that Google's popular Gmail service "was actively violating the privacy of its users by displaying ads related to keywords in their email," according to the company's website.

The company's small number of developers constructed a "highly convoluted" encryption of mail stored on Lavabit's servers, making mail inaccessible even to Lavabit employees. According to the company, this "ultimately makes it a massive pain in the rear for agencies like the NSA to decrypt."

"In theory, an attack with unlimited computing resources could use brute force to decipher the original message", the company noted, but "in practice, the key lengths Lavabit has chosen equal enough possible inputs that a brute force attack shouldn't be feasible for a long time to come."

The decision by Lavabit was followed by an announcement from Silent Circle, which offers a range of secure communication services, that it was pulling out of email provision entirely. Silent Circle was co-founded by Phil Zimmerman, the developer of PGP encryption software. According to a statement from the company, it had not yet been contacted by US law enforcement agencies, but "could see the writing on the wall." It suspended email because it could not guarantee security of its managed encryption service, in which Silent Circle handled encryption keys and certificates for its users.

In fact, Silent Circle explained, the SMTP, POP3 and IMAP protocols in use for email cannot be secure. These protocols necessarily generate metadata on senders, recipients and timestamps for every single email created, even if the content itself is encrypted.

Silent Circle explained that it intended to continue offering secure phone, video and text services with full end to end encryption.

In the end, there can be no technical fix for the turn by the world's leading capitalist powers to saturation digital surveillance. The internet and related technologies point to the astonishingly progressive possibilities opened up by modern communications technology. But at the behest of a narrow super-rich minority, this is being utilized as a vast digital surveillance network where every action can be saved by the authorities for current and future targeting and repression.

Snowden's actions generated mass outrage at the extent of the operations he revealed. Opinion polls have consistently sided with Snowden against the US government. The response from the US government, however, has been to escalate its assault on free communications.

The turn to police states and universal surveillance can only be opposed by the transformation of popular anger at spying into a political mobilisation of working people in a struggle for world socialism. Only on this basis can democratic rights be preserved, expanded and modern technology used to advance the interests of all humanity.

To contact the WSWS and the Socialist Equality Party visit:

wsws.org/contact

© World Socialist Web Site