Bruce Schneier

Schneier on Security

A blog covering security and security technology.

« How Many Leakers Came Before Snowden? | Main

August 30, 2013

More on the NSA Commandeering the Internet

If there's any confirmation that the U.S. government has commandeered the Internet for worldwide surveillance, it is what happened with Lavabit earlier this month.

Lavabit is -- well, was -- an e-mail service that offered more privacy than the typical large-Internet-corporation services that most of us use. It was a small company, owned and operated by Ladar Levison, and it was popular among the tech-savvy. NSA whistleblower Edward Snowden among its half-million users.

Last month, Levison reportedly received an order -- probably a National Security Letter -- to allow the NSA to eavesdrop on everyone's e-mail accounts on Lavabit. Rather than "become complicit in crimes against the American people," he turned the service off. Note that we don't know for sure that he received a NSL -- that's the order authorized by the Patriot Act that doesn't require a judge's signature and prohibits the recipient from talking about it -- or what it covered, but Levison has said that he had complied with requests for individual e-mail access in the past, but this was very different.

So far, we just have an extreme moral act in the face of government pressure. It's what happened next that is the most chilling. The government threatened him with arrest, arguing that shutting down this e-mail service was a violation of the order.

There it is. If you run a business, and the FBI or NSA want to turn it into a mass surveillance tool, they believe they can do so, solely on their own initiative. They can force you to modify your system. They can do it all in secret and then force your business to keep that secret. Once they do that, you no longer control that part of your business. You can't shut it down. You can't terminate part of your service. In a very real sense, it is not your business anymore. It is an arm of the vast U.S. surveillance apparatus, and if your interest conflicts with theirs then they win. Your business has been commandeered.

For most Internet companies, this isn't a problem. They are already engaging in massive surveillance of their customers and users -- collecting and using this data is the primary business model of the Internet -- so it's easy to comply with government demands and give the NSA complete access to everything. This is what we learned from Edward Snowden. Through programs like PRISM, BLARNEY and OAKSTAR, the NSA obtained bulk access to services like Gmail and Facebook, and to Internet backbone connections throughout the US and the rest of the world. But if it were a problem for those companies, presumably the government would not allow them to shut down.

To be fair, we don't know if the government can actually convict someone of closing a business. It might just be part of their coercion tactics. Intimidation, and retaliation, is part of how the NSA does business.

Former Qwest CEO Joseph Nacchio has a story of what happens to a large company that refuses to cooperate. In February 2001 -- before the 9/11 terrorist attacks -- the NSA approached the four major US telecoms and asked for their cooperation in a secret data collection program, the one we now know to be the bulk metadata collection program exposed by Edward Snowden. Qwest was the only telecom to refuse, leaving the NSA with a hole in its spying efforts. The NSA retaliated by canceling a series of big government contracts with Qwest. The company has since been purchased by CenturyLink, which we presume is more cooperative with NSA demands.

That was before the Patriot Act and National Security Letters. Now, presumably, Nacchio would just comply.

Protection rackets are easier when you have the law backing you up.

As the Snowden whistleblowing documents continue to be made public, we're getting further glimpses into the surveillance state that has been secretly growing around us. The collusion of corporate and government surveillance interests is a big part of this, but so is the government's resorting to intimidation. Every Lavabit-like service that shuts down -- and there have been several -- gives us consumers less choice, and pushes us into the large services that cooperate with the NSA. It's past time we demanded that Congress repeal National Security Letters, give us privacy rights in this new information age, and force meaningful oversight on this rogue agency.

This essay previously appeared in USA Today.

Tags: essays, FBI, internet, National Security Letters, national security policy, NSA, PATRIOT Act, privacy, surveillance, whistleblowers
Posted on August 30, 2013 at 6:12 AM • 24 Comments

To receive these entries once a month by e-mail, sign up for the Crypto-Gram Newsletter.

Like Tweet +1 Share Submit

Comments

sshdoor • August 30, 2013 7:08 AM

Time to change the ssh protocol so that the clear-text password is not more given to the Daemon sshd.

For this, it is not necessary need to change passwords, or salting mechanism of /etc/shadow (unlike the patch Secure Remote Password (SRP) for openssh):

the bcrypt call should be done by the client ssh, not by the server sshd.

(now, sshd has clear-text access on your password as you typed it; it even know if and how you mis-spelled it).

Quantum Mechanic • August 30, 2013 7:12 AM

Presumably, if forced to keep the business running, there are alternatives such as charging a ridiculous service fee, selling the business to your new company in NZ, or having your security fall over and get hacked.

Does anyone have a scheme outlined for multi-jurisctional distributed service, such that complying with an NSL-type request in one jurisdiction gracefully removes itself from that jurisdiction just by turning on surveillance? Is there a cute name for such behavior?

---

phred14 • August 30, 2013 7:30 AM

What I find far more disturbing is the disappearance of Groklaw - a weblog that started with the SCO-Linux lawsuits and moved on to other checks on corporate/legal behavior. Groklaw has shut down, with essentially the same citation as LavaBit and the other, name forgotten, secure email service.

I find it more disturbing because it implies a tit-for-tat between government and big business - You let us peek, and we'll protect you from corporate whistleblowers. I'm not saying shutting down LavaBit was right - it wasn't, but at some level it could be taken (or mistaken) as national-security related. Nothing of the sort can be said for Groklaw - it's pure and simple corporate protection - or corruption.

---

michael • August 30, 2013 7:34 AM

I was wondering if you could structure a company like Lavabit in such a way that all customers receive an ownership share in the company and write the bylaws of the company so that all owner-clients have the right to