The lawyers for the Internet Archive asked to have a private meeting, with no one else there but me. And they said, we've just received a national-security letter, to find out a lot of detailed information about a patron of the Internet Archive.

They were sort of grim: "Let's lock the doors, you'll be the only person who hears about this." They said that, according to the law, you have to give them the information they want, and you can only talk to people such that you can fulfill this request. Other than that, there's nothing else you can do, and then you can't ever mention it to anybody, ever.

So I asked, "Can I bring this up with my board?" And the answer is no. Could I discuss it with my wife? The answer is no, not without risking being put in prison for years.

Then the lawyers said the only thing you can do — and there's a risk to it — is to challenge it in court: sue the U.S. government. There is no appeals process; there is no discussion. The only thing you can do is to sue them. As I understand it, that leads to a delay, and that only makes you [look] more guilty of whatever it is they want to accuse you of, should you lose. You're going into risky territory, just by not complying and not shutting up about it.

My Fellow Users,

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. 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. …

Sincerely,

Ladar Levison

Owner and Operator, Lavabit LLC

NSL FAQ @ EFF

- https://www.eff.org/issues/national-security-letters/faq

A guide to FISA @ PI

- https://www.privacyinternational.org/blog/a-guide-to-fisa-ss1881a-the-law-behind-it-all

NSA "SMS: A Goldmine" slides

- http://cryptome.org/2014/01/nsa-sms-exploit.pdf
- 8 pages were released. circ. 2011.
- 6.1 trillion messages a year in 2010
- “Typed” Text Message (p. 4)
- contact chaining, geolocation, alternative identifiers, travel, finance (p. 5)
- 200 millions SMS per day (70 billions per year, about 1%-2% of the total volume worldwide).
- Technical details in p. 8

NSA PRISM Slides

- https://archive.org/details/NSA-PRISM-Slides

PRISM (surveillance program)

- http://en.wikipedia.org/wiki/PRISM_%28surveillance_program%29

Microsoft: "We provide customer data only when we receive a legally binding order or subpoena to do so, and never on a voluntary basis. In addition we only ever comply with orders for requests about specific accounts or identifiers. If the government has a broader voluntary national security program to gather customer data we don't participate in it."

Yahoo!: "Yahoo! takes users' privacy very seriously. We do not provide the government with direct access to our servers, systems, or network."[120] "Of the hundreds of millions of users we serve, an infinitesimal percentage will ever be the subject of a government data collection directive."

Facebook: "We do not provide any government organization with direct access to Facebook servers. When Facebook is asked for data or information about specific individuals, we carefully scrutinize any such request for compliance with all applicable laws, and provide information only to the extent required by law."

Google: "Google cares deeply about the security of our users' data. We disclose user data to government in accordance with the law, and we review all such requests carefully. From time to time, people allege that we have created a government ‘back door' into our systems, but Google does not have a backdoor for the government to access private user data." "[A]ny suggestion that Google is disclosing information about our users' Internet activity on such a scale is completely false."

Apple: "We have never heard of PRISM. We do not provide any government agency with direct access to our servers, and any government agency requesting customer data must get a court order."

Dropbox: "We've seen reports that Dropbox might be asked to participate in a government program called PRISM. We are not part of any such program and remain committed to protecting our users' privacy."

Upstream collection

- http://en.wikipedia.org/wiki/Upstream_collection
- Upstream collection programs allow access to very high volumes of data. A first pre-selection is done by the telecommunication providers themselves, who select the internet traffic that most likely contains foreign communications. Then the data is passed on to the NSA, where a second selection is made by briefly copying the traffic and filtering it by using so-called "strong selectors" like phone numbers, e-mail or IP addresses of people and organizations which NSA is interested in.

“ToS;DR” Classification & Rating

- http://tosdr.org/classification.html

- Google http://tosdr.org/#google
- DuckDuckGo http://tosdr.org/#duckduckgo

- Law and gov request http://tosdr.org/topics.html#law-gov
- Personal Data http://tosdr.org/topics.html#personal-data
- Anonymity and tracking http://tosdr.org/topics.html#track

Google's Transparency Report

- User Data Request
  - http://www.google.com/transparencyreport/userdatarequests/
- Taiwan
  - http://www.google.com/transparencyreport/userdatarequests/TW/
- US
  - http://www.google.com/transparencyreport/userdatarequests/US/
- China
  - http://www.google.com/transparencyreport/userdatarequests/CN/