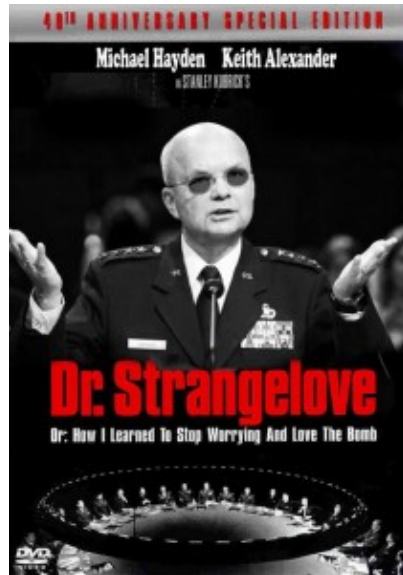


LAVABIT AND THE DEFINITION OF US GOVERNMENT HUBRIS



Graphic by Darth

Well, you know, if you do not WANT the United States Government sniffing in your and your family's underwear, it is YOUR fault. Silly American citizens with your outdated stupid piece of paper you call the Constitution.

Really, get out if you are a citizen, or an American communication provider, that actually respects American citizen's rights. These trivialities the American ethos was founded on are "no longer operative" in the minds of the surveillance officers who claim to live to protect us.

Do not even think about trying to protect your private communications with something so anti-American as privacy enabling encryption like Lavabit which only weakly, at best, even deigned to supply.

Any encryption that is capable of protecting an American citizen's private communication (or

even participating in the TOR network) is essentially inherently criminal and cause for potentially being designated a “selector”, if not target, of any number of searches, whether domestically controlled by the one sided ex-parte FISA Court, or hidden under Executive Order 12333, or done under foreign collection status and deemed “incidental”. Lavabit’s Ladar Levinson knows.

Which brings us to where we are today. Let Josh Gerstein set the stage:

A former e-mail provider for National Security Agency leaker Edward Snowden, Lavabit LLC, filed a legal brief Thursday detailing the firm’s offers to provide information about what appear to have been Snowden’s communications as part of a last-ditch offer that prosecutors rejected as inadequate.

The disagreement detailed in a brief filed Thursday with the U.S. Court of Appeals for the Fourth Circuit resulted in Lavabit turning over its encryption keys to the federal government and then shutting down the firm’s secure e-mail service altogether after viewing it as unacceptably tainted by the FBI’s possession of the keys.

I have a different take on the key language from Lavabit’s argument in their appellate brief though, here is mine:

First, the government is bereft of any statutory authority to command the production of Lavabit’s private keys. The Pen Register Statute requires only that a company provide the government with technical assistance in the installation of a pen- trap device; providing encryption keys does not aid in the device’s installation at all, but rather in its use. Moreover, providing private keys is not “unobtrusive,” as

the statute requires, and results in interference with Lavabit's services, which the statute forbids. Nor does the Stored Communications Act authorize the government to seize a company's private keys. It permits seizure of the contents of an electronic communication (which private keys are not), or information pertaining to a subscriber (which private keys are also, by definition, not). And at any rate it does not authorize the government to impose undue burdens on the innocent target business, which the government's course of conduct here surely did.

Second, the Fourth Amendment independently prohibited what the government did here. The Fourth Amendment requires a warrant to be founded on probable cause that a search will uncover fruits, instrumentalities, or evidence of a crime. But Lavabit's private keys are none of those things: they are lawful to possess and use, they were known only to Lavabit and never used by the company to commit a crime, and they do not prove that any crime occurred. In addition, the government's proposal to examine the correspondence of all of Lavabit's customers as it searched for information about its target was both beyond the scope of the probable cause it demonstrated and inconsistent with the Fourth Amendment's particularity requirement, and it completely undermines Lavabit's lawful business model. General rummaging through all of an innocent business' communications with all of its customers is at the very core of what the Fourth Amendment prohibits.

The legal niceties of Lavabit's arguments are thus:

The Pen Register Statute does not come close. An anodyne mandate to provide information needed merely for the “unobtrusive installation” of a device will not do. If there is any doubt, this Court should construe the statute in light of the serious constitutional concerns discussed below, to give effect to the “principle of constitutional avoidance” that requires this Court to avoid constructions of statutes that raise colorable constitutional difficulties. *Norfolk S. Ry. Co. v. City of Alexandria*, 608 F.3d 150, 156–57 (4th Cir. 2010).

And, later in the pleading:

By those lights, this is a very easy case. Lavabit’s private keys are not connected with criminal activity in the slightest—the government has never accused Lavabit of being a co-conspirator, for example. The target of the government’s investigation never had access to those private keys. Nor did anyone, in fact, other than Lavabit. Given that Lavabit is not suspected or accused of any crime, it is quite impossible for information known only to Lavabit to be evidence that a crime has occurred. The government will not introduce Lavabit’s private keys in its case against its target, and it will not use Lavabit’s private keys to impeach its target at trial. Lavabit’s private keys are not the fruit of any crime, and no one has ever used them to commit any crime. Under those circumstances, absent any connection between the private keys and a crime, the “conclusion[] necessary to the issuance of the warrant” was totally absent. *Zurcher*, 436 U.S., at 557 n.6 (quoting, with approval, Comment, 28 U. Chi. L. Rev. 664, 687 (1961)).

What this boils down to is, essentially, the government thinks the keys to Lavabit's encryption for their customers belong not just to Lavabit, and their respective customers, but to the United States government itself.

Your private information cannot be private in the face of the United States Government. Not just Edward Snowden, but anybody, and everybody, is theirs if they want it. That is the definition of bullshit.

[Okay, big thanks to Darth, who generously agreed to let us use the killer Strangelovian graphic above. Please follow Darth on Twitter]