GlobalResearch
Center for Research on Globalization

The Police State Wants What The Police State Wants

The FBI went after Levision's secure email service called Lavabit. The NSA and the rest of the security state couldn't get into it.

By William Boardman
Global Research, October 20, 2013
Reader Supported News

Region: USA
Theme: Law and Justice, Police State & Civil Rights

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." The Fourth Amendment of the U. S. Constitution

The founding document of the United States is inherently suspicious of a government's willingness to abuse its powers, a suspicion rooted in centuries of tyranny around the world. Even the U.S. government, as well as state and local governments, have abused their powers from time to time since the country's beginning. The drift toward an American police state intensified under the guise of anti-Communism, but that was mostly a convenient cover for state intrusion into people's lives. The Soviet Union collapsed, but the nascent American police state kept growing. The Patriot Act of 2001, a massive assault on personal and political liberty, was largely written before 9/11 and passed, largely unexamined, in the hysterical atmosphere and raw panic of that over-hyped "new Pearl Harbor."

Now we have a police state apparatus of almost unimagined dimension, most of which is kept secret and remains unknown, despite the efforts of a few reporters and whistle blower, who tell the truth at their personal peril.

The "American police state" is likely an abstraction in the minds of many people, and as long as they remain unknowing and passive, it's likely to leave them alone. But even law-abiding innocence is not a sure protection of a person's right to be secure. And when the police state comes after you in one of its hydra-headed forms, the assault can be devastating.

For starters, the state won't always tell you when it begins

The intrusion of the police state into your life can shatter your world even before you realize it's begun. Fight it, or surrender to it, the cost is huge. Recovery may be possible, eventually, if it's ever allowed, but it will be hard, and it will take time.

In May 2013, Ladar Levison was 32 when the police state first came after him. The dreaded "knock on the door" was actually only an FBI business card on his door at home. And Levison's initial interactions with the FBI were reportedly mild and civil, at first by email and later in person. The FBI was interested in Levision because he owned and operated a secure

email service called Lavabit. From the FBI point of view, Lavabit was *too* secure, because the NSA and the rest of the security state couldn't get into it.

Right out of college, Levison had started Lavabit as a sole proprietorship in April 2004 (the same month Google launched Gmail at a much greater scale). Having grown up in San Francisco, Levison studied computer science at Southern Methodist University in Dallas, where he still lives. While working on his start-up, he supported himself mostly with internet security projects for financial services. He also worked as a consultant on website development for clients such as Dr Pepper, Nokia, and Adidas.

What Lavabit was selling was secure email, much more secure than anything Google, Microsoft, or most other email providers were offering. The demand was not that great at first. It took six years for Lavabit to gather enough paying subscribers to allow Levison to devote himself to the business fulltime in 2010. Even when the FBI became interested in Lavabit in May 2013, it was still a small company, with two employees and about 400,000 subscribers. But one of those subscribers was another American about Levison's age, 30-year old Edward Snowden, the whistleblower whose leaked documents have added so much to our understanding of the dimensions and activities of the American police state. Snowden opened his edsnowden@lavabit.com email account in 2010.

Political repression may not be the government's overt intent, but it works

At this point, there's no indication that Levison and Lavabit ever had anything but a commercial relationship with Snowden. It's even possible that Snowden had nothing to do with the FBI's initial interest in Lavabit. It may be that Lavabit's effective security was sufficient offense to the surveillance forces to make it an object of attack for its own sake. In May 2013, Levison says he had the impression the FBI agents who talked to him didn't even know who or what was the subject of their investigation. The FBI hasn't said.

Levison is not an obviously political person, he hasn't been revealed to be involved in party politics or political causes. "Until last summer, Mr. Levison, a Republican of libertarian leanings, had not been active in politics," according to the New York Times October 9. He seems to be the person he seems to be: a thoughtful, hardworking, physically fit, computer business guy who has had a dog named Princess since January 2010 and who spends a lot of his spare time keeping in shape playing beach volleyball.

Princess has her own album on his Facebook page, where the dominant theme by far is Levison's competition in beach volleyball (with albums for Sunday Night, as well as Monday, Tuesday, Wednesday, and Thursday Nights) and there is one picture of Levison with Rep. Ron Paul. Levison's page shows membership in just one Facebook group, "OCCUPY (Support) EDWARD SNOWDEN and All Other Whistleblowers," to which someone else added him about two months ago. Among his 43 "Likes," Levison lists two Interests (programming and computers), lots of volleyball Activities, and six books, including William Gibson's "Neuromancer," George Orwell's "1984," and Dostoevski's "Crime and Punishment."

From another perspective, Levison is as political as the Fourth Amendment, which is as profoundly political as it gets. It was the Patriot Act's assault on the Fourth Amendment, Levison says, that contributed to his decision to start Lavabit in 2004, when the act was up for renewal and much in the news. Among the many objections to the act was that it gave to federal agents excessive authority to, in effect, write their own search warrants on no other authority but their own. In the Orwellian language of the act, these personal searched

warrants are known as “national security letters.” Levison designed the security architecture of the Lavabit email and storage services to be beyond the reach of unwarranted searches, even in national security letters. As Levison recalled on Democracy NOW! in August:

> “And as I was designing and developing the custom platform, it was right around when the PATRIOT Act came out. And that’s really what colored my opinion and my philosophy, and why I chose to take the extra effort and build in the secure storage features and sort of focus on the privacy niche and the security focus niche…. [for] people who want email but don’t necessarily want it lumped in and profiled along with their searches or their browsing history or any of their other Internet activities.”

You can’t reveal what you don’t know – and that provides more security

During May 2013, Levison met for “a couple hours” with FBI agents at his office, where he explained how his security system and his business operated. As Levison told Democracy NOW! the service included his personal pledge of security:

> “I’ve always liked to say my service was by geeks, for geeks. It’s grown up over the last 10 years, it’s sort of settled itself into serving those that are very privacy-conscious and security-focused. We offered secure access via high-grade encryption. And at least for our paid users, not for our free accounts—I think that’s an important distinction—we offered secure storage, where incoming emails were stored in such a way that they could only be accessed with the user’s password, so that, you know, even myself couldn’t retrieve those emails.
>
> “And that’s what we meant by encrypted email. That’s a term that’s sort of been thrown around because there are so many different standards for encryption, but in our case it was encrypted in secure storage, because, as a third party, you know, I didn’t want to be put in a situation where I had to turn over private information. I just didn’t have it. I didn’t have access to it.”

Over the years, Lavabit has received and complied with “at least two dozen subpoenas” from the local sheriff’s office to the federal courts, Levison says, “I’ve always complied with the law.” Each of those subpoenas targeted a specific individual and appeared to Levison to be consistent with the Fourth Amendment. As recently as June 2013, he complied with an unrelated subpoena seeking information on one of his subscribers accused of violating child pornography law.

A secret subpoena from the American police state is different

On June 6, 2013, the Guardian began publishing surveillance state revelations based on documents from Edward Snowden, the Lavabit.com email subscriber. On June 9, Snowden revealed that he was the whistlblower who leaked documents to the Guardian and others. The first secret court order against Lavabit came the next day.

On or about June 10, the Justice Dept., on behalf of the FBI, went to federal court to compel Lavabit to provide information “relevant and material to an ongoing criminal investigation” involving someone with a single Lavabit email account. The FBI has not identified the subject of this investigation, but it is widely believed to be Snowden.

The United States District Court for the Eastern District of Virginia (the Fourth Circuit) granted the FBI's request and issued the disclosure order against Lavabit that same day. A one-page, single-spaced attachment to the order listed the categories of information to be disclosed, including names, addresses, phone records, other subscriber identities, billing records, activity records, and "information about each communication" – in other words, everything about the email account "not including the contents of communications." The order did not mention encryption keys, SSL keys, or the like. These are closely guarded secrets in a security business like Lavabit.

The U.S. Magistrate Judge who signed the initial order gave Lavabit 10 days to comply. He also sealed the court records from public view and further ordered that Lavabit "shall not disclose the existence of the application of the United States, or the existence of this order" to anyone except "an attorney for Lavabit." In other words, Levison was subject to a gag order before he ever found out the FBI was definitely coming after him.

In the meantime, on June 14, the Justice Dept. filed a sealed criminal complaint against Snowden, who was then in Hong Kong. The government accused him of three offenses – theft of government property and two forms of "unauthorized communication" the Espionage Act of 1917. The criminal complaint, which was made public a week later, gave the government 60 days to file a formal indictment.

Getting unsatisfying compliance, the FBI decided to raise the stakes

According to a later Justice Dept. filing: "Mr. Levison received that order on June 11, 2013. Mr. Levison responded by mail, which was not received by the government until June 27, 2013. Mr. Levison provided *very little* of the information sought…." [emphasis added]

On June 28, the day after getting Levison's belated response to the June 10 order, the Justice Dept. went back to the Fourth Circuit Court in Alexandria seeking an order "authorizing the installation and use of a pen register/trap device on an electronic mail account" – an FBI wiretap on email. Levison had no notice of the government motion and no opportunity to contest it. A new judge on the case, Magistrate Judge Theresa Buchanan, promptly ordered the wiretap installed on the basis that the government "has certified that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation…." Like the first order, this order did not mention encryption keys, SSL keys, or the like.

FBI special agents met with Levison in Dallas the same day to discuss the new order, which Levison had not yet received, as well as a prior summons to appear before a grand jury. The agents presumably explained to Levison that the court had issued a secret order based on a secret motion, itself based on secret evidence (or none at all) and that Levison was not only compelled to comply but was also still under court order to keep the whole secret process a secret, this time with no exception even for his attorney.

According to a later government filing, "Mr. Levison told the agents that he would not comply with the pen register order and wanted to speak to an attorney. It was unclear whether Mr. Levison would not comply with the order because it was technically not feasible or difficult or was not consistent with his business practice of providing secure, encrypted email service for his customers."

As Levison months later explained to reporters about Lavabit: "We're wholly focused on

secure email. Without it, we have no business." In Levison's view, breaking Lavabit's security without the right to tell his customers would have been to commit commercial fraud.

Judge Buchanan keeps the pressure on Levison and Lavabit

Following this meeting, the Justice Dept. immediately went before Judge Buchanan seeking an order to compel Lavabit to comply with the other Magistrate's earlier order and install the FBI wiretap and to "furnish agents from the Federal Bureau of Investigation, forthwith, all information, facilities, and technical assistance necessary to accomplish the installation and use of the pen/trap device…" as ordered pursuant to federal law [U.S. Code, Title 18, sec. 3123].

Judge Buchanan immediately granted the "Order Compelling Compliance Forthwith," based in part on her findings that "Lavabit informed the Federral Bureau of Investigation that the user of the account had enabled Lavabit's encryption services and thus the pen/trap device would not collect the relevant information" and that "Lavabit informed the FBI that it had the technological capability to obtain the information but did not want to 'defeat [its] own system'…"

Judge Buchanan ordered Lavabit to provide "unencrypted data pursuant to the Order." Noting that failure to comply "forthwith" would subject Lavabit to "any penalty within the power of the court," Judge Buchanan added in her own handwriting, "including the possibility of criminal contempt of court." This order was issued under seal.

Previously, Levison faced the possibility of being fined for civil contempt if he failed to comply. Now he also faced going to jail. And the court's most recent orders, in their plain language, prevented Levison from discussing his situation with anyone, not even an attorney.

According to the FBI, agents "made numerous attempts, without success, to speak and meet directly with Mr. Levison" during the next ten days. On July 9, the Justice Dept. returned to the Fourth Circuit court seeking an order for Lavabit to show cause why it "has failed to comply with the orders entered June 29" by Magistrate Buchanan, and why Lavabit should not be held in contempt of court for its failure to comply.

Judge Hilton decides a hearing with the parties present might help

Judge Claude Hilton issued the show cause order the same day, including a summons for Lavabit to appear at a hearing a week later. Judge Hilton is a secrecy case veteran, having served on the secretive FISA (Foreign Intelligence Surveillance Act) court from 2000 to 2007. The Judge continued to keep the Lavabit case under seal, but reinstated Lavabit's exception to the gag rule when consulting with an attorney.

The next day, Levison went to the FBI field office in Dallas for a meeting/conference call that included prosecutors and FBI agents in Washington and his attorney in San Francisco, convened "to discuss Mr. Levison's questions and concerns… [that] focused primarily on how the pen register device would be installed on the Lavabit LLC system, what data would be captured by the device, what data would be viewed and preserved by the government… [and] whether Mr. Levison would be able to provide 'keys' for encrypted information."

The parties did not reach an agreement at the meeting and the next day, July 11, Levison's

attorney informed the FBI that she no longer represented Levison or Lavabit. The same day, Levison "indicated that he would not come to court [for the July 16 show cause hearing] unless the government paid for his travel," according to a government filing.

Rather than engage in a dispute over travel expenses, the FBI served Levison with a subpoena to appear before a Fourth Circuit grand jury, also on July 16. The government is responsible for the travel arrangements of grand jury witnesses, and the FBI so advised Levison by email. The grand jury subpoena left little wriggle room in its effort to force Lavabit to surrender the encryption keys that were essential to its business:

> "In addition to your personal appearance, you are directed to bring to the grand jury the public and private encryption keys used by lavabit.com in any SSL (Secure Socket Layer) or TLS (Transport Security Layer) sessions, including HTTPS sessions with clients using lavabit.com website and encrypted SMTP communications (or Internet communications using other protocols) with mail servers;
>
> "Any other information necessary to accomplish the installation and use of the pen/trap device ordered by Judge Buchanan on June 28…."

"I don't trust you, but you should trust me" and vice-versa

Levison responded on July 13 with an email to the U.S. Attorney's office, offering an alternative to the FBI-operated wiretap. Levison proposed that he would collect the court-designated data himself. While he didn't state it in the email, this would address one of Levison's primary concerns, that there was no effective oversight to prevent the FBI from gathering more data than the court had allowed. Levison proposed to design and implement the solution, gather the data manually, and provide it to the FBI at the end of the 60-day court order – for a price of $2,000. For another $1,500, he offered to provide data "more frequently," which would require implementing an automated system.

The U.S. Attorney chose not to explore the offer. In a brusque and internally contradictory reply email the same day, an assistant U.S. Attorney explained "that the proposal was inadequate because, among other things, it did not provide for real-time transmission of results, and it was not clear that Mr. Levison's request for money constituted the 'reasonable expenses' authorized by the statute." The government later admitted to the court that it was "unclear" as to precise details of the proposal. The clear implication of Levison's proposal is a willingness to provide real-time transmission for reasonable compensation. But that would leave Levison in control. The government didn't consider that a useful compromise.

On July 15, Levison flew to Washington for his show cause hearing at 10 the next morning, although he thought it was set for 10:30 and arrived late. He was appearing *pro se,* representing himself without an attorney.

Even a federal court hearing can be a comedy of errors

The government goal for the July 16 hearing remained unchanged: "Lavabit LLC may comply with the pen register order by simply allowing the FBI to install the pen register devise and provide the FBI with the encryption keys." Lacking compliance, the government asked the court to impose a civil contempt sanction of $1,000 a day until Lavabit complied.

The government also requested a search warrant for the encryption keys. Judge Hilton granted the search warrant before the hearing began.

As it turned out, the 20-minute hearing resulted in no change in the legal standing of the parties, but did produce a transcript with moments of unintentional hilarity.

Present in the courtroom were Judge Hilton and the court staff. U.S. Attorney James Trump represented the government, along with three other lawyers and an FBI agent. Levison was alone.

The U.S. Attorney wanted to know if Levison was going to comply with the wiretap order, but Judge Hilton wouldn't ask and Levison wouldn't say. Or rather, Levison said he had always been ready and willing to comply with installation of the wiretap, but he was reluctant to give up the encryption codes, which would give the FBI access to all 400,000 of his subscribers even though the court order named only one. "There was never an explicit demand that I turn over those keys," Levison said.

The U.S. Attorney argued that Judge Buchanan had effectively if not specifically ordered Levison to turn over the encryption keys. Judge Hilton wasn't touching that: "I'm not sure I ought to be enforcing Judge Buchanan's order." Judge Hilton said that his order was to install the wiretap and Levison had said he'd do that, so – "You're trying to get me to deal with a contempt before there's any contempt, and I have a problem with that."

Levison moved to unseal all but the sensitive information in the proceedings. Judge Holton denied the motion, based on the underlying criminal investigation. Levison asked the judge to order "some sort of external audit to ensure that your oders are followed to the letter" as to FBI data collection. The judge refused. Levison moved to continue the hearing to allow him to retain counsel. Judge Hilton granted the continuance.

Levison and Lavabit get legal representation from a Virginia firm

Levison's new attorney is Jesse Binnall of Bronley & Binnall PLLC in Fairfax, Virginia. Binnall, 34, was a communication major at George Mason University and graduated from the Law School there in 2009. Binnall and Levison would later be among the first guests on the New Ron Paul Channel in mid-August.

On July 25, Binnall filed under seal a "Motion to quash" the outstanding grand jury subpoena and the search warrant against Lavabit. The motion requested "that this Court direct that Lavabit does not have to produce its Master Key. Alternatively, Lavabit and Mr. Levinson request that they be given an opportunity to revoke the. current encryption key and reissue a new encryption key at the Government's expense. Lastly, Lavabit and Mr. Levinson request that, if they are required to produce the Master Key, that they be reimbursed for its costs which were directly incurred in producing the Master Key…."

In support of his motion, Binnall made a number of arguments against the actions of the government, which had not faced serious legal opposition up to this point.

Binnall pointed out that giving the government access to Lavabit's Master Key is tantamount to giving the government access to all of Lavabit's 400,000 users. That amounts to a general warrant that is unconstitutional, Binnall wrote, and:

> "It is axiomatic that the Fourth Amendment prohibits general warrants [with Supreme Court cases cited]…. The Fourth Amendment's particularity requirement is meant to 'prevent the seizure of one thing under a warrant describing another' [citation omitted]. This is precisely the concern with the Lavabit Subpoena and Warrant and, in this circumstance, the particularity requirement will not protect Lavabit. By turning over the Master Key, the Government will have the ability to search each and every 'place,' 'person [and] thing' on Lavabit's network…. Additionally, the Government has no probable cause to gain access to the other users accounts."

The government seemed unconcerned about Levison's business survival

Bindall also argued that the court should quash the subpoena and search warrant as creating an "undue burden" on Lavabit as defined by law [U.S. Code Title 18, sec. 2703]:

> "Not only has Lavabit expended a great deal of time and money in attempting to cooperate with the Government thus far, but, Lavabit will pay the ultimate price –the loss of its customers' trust and business – should the Court require that the Master Key be turned over. Lavabit's business, which is founded on the preservation of electronic privacy, could be destroyed if it is required to produce its Master Key."

Also on July 25, Binnall filed a motion to unseal court records and to lift the gag order on his client, since the "gag order infringes upon freedom of speech under the First Amendment, and should he subjected to constitutional case law. "

Unsurprisingly, the U.S. Attorney filed a motion in opposition.

At the motion hearing on August 1, Judge Hilton engaged in lengthy colloquy with attorney Binnall. Before the 25-minute hearing was half over, the judge had denied both motions and the U.S. Attorney had said little more than "Good morning." Judge Hilton gave Levison and Lavabit until 5 p.m. Dallas time on August 2 to comply.

Levison's compliance took an unexpected form

The next day in Dallas, at about 1:30 p.m., Levison provided information that purported to be full compliance with the court's orders. Whether it was actual compliance remains uncertain. The government was not happy and engaged with attorney Binnall to achieve satisfactory compliance, without success. On August 5 the government filed a motion for sanctions against Levison, calling his apparent compliance "unworkable" and describing it as follows:

> "Mr. Levison gave the FBI a printout of what he represented to be the encryption keys needed to operate the pen register. This printout, in what appears to be 4-point type, consists of 11 pages of largely illegible characters. See Attachment A. (The attachment was created by scanning the document provided by Mr. Levison; the original document was described by the Dal!as FBI agents as slightly clearer than the scanned copy but nevertheless illegible.) Moreover, each of the five encryption keys contains 512 individual characters – or a total of 2560 characters. To make use of these keys, the FBI would have to manually input all 2560 characters, and one incorrect keystroke in this laborious process would render the FBI collection system incapable of collecting decrypted data."

When this compliance effort became public two months later, TechCrunch called it “an epic troll.” At the time, the government was not amused and called for the court to sanction Levison $5,000 a day, beginning at noon August 5. The court promptly granted the motion, while reminding the parties that all aspects of the matter remained under seal. Known only to the participants and some court employees, the case was still unknown to the public.

Levison makes a tantalizing public announcement

That secrecy ended on August 8, when Ladar Levison shut down Lavabit, posting a short notice on the Lavabit.com website, together with a link to the Lavabit Legal Defense Fund. As Levison explained:

> “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.
>
> “What’s going to happen now? We’ve already started preparing the paperwork needed to continue to fight for the Constitution in the Fourth Circuit Court of Appeals. A favorable decision would allow me resurrect Lavabit as an American company.
>
> “This experience has taught me one very important lesson: 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.”

Also on August 8, Levison fully complied with the Fourth Circuit courts orders, turning over the encryption keys to a now defunct service. He had incurred 2 days of sanctions – owing the government $10,000 – which remains pending.

The next day, Silent Circle, a global encrypted communications service, stayed in business but preemptively wiped out its email service (about 5 per cent of its customers) in anticipation of a government request that the company wouldn’t want to have to obey. “Meanwhile, Silent Circle is working on replacing its defunct e-mail service with a system that doesn’t rely on traditional e-mail protocols and keeps no messages or metadata within the company’s grasp. It is based on a protocol often used for instant messages and other applications. [CEO Mike] Janke says the goal is for this to not be e-mail, but ‘for all intents and purposes it looks, feels, and acts like e-mail,’” according to MIT Technology Review.

Lavabit’s closing drew some news coverage over the next week, but any story was hampered by the gag order that severely limited what Levison and Binnall could safely say. As Levison told Forbes the day after shutting down Lavabit:

> “This is about protecting all of our users, not just one in particular. It’s not my place to decide whether an investigation is just, but the government has the legal authority to force you to do things you’re uncomfortable with.…The fact that I can’t talk about this is as big a problem as what they asked me to do.…

> The methods being used to conduct those investigations should not be secret."

The FBI and the Justice Dept. Have not commented publicly about the Lavabit case beyond their court filings.

Being secret, federal court appeal gets no news coverage

On August 15, Lavabit attorney Binnall filed notice – under seal – that he was appealing the federal district court's rulings of August 1 and August 5 to the United States Court of Appeals for the Fourth Circuit. In other words, the government can not only keep the public ignorant of what it's doing, it can also prevent the public from knowing that anyone objects to the government's actions as unconstitutional.

In the Lavabit case, at least, this changed abruptly on October 2, when Judge Claude Hilton ordered a censored version of 23 documents (162 pages) made public. The redactions in these documents appear, from context, to be intended mostly to conceal details of the criminal investigation into Snowden or some other lavabit.com user. Since the unsealing of the court documents, news coverage had expansed, and Levison and Binnall have appeared in public across the country to argue their cause. As Levison put it on his Facebook page October 2:

> "If the Obama administration feels compelled to continue violating the privacy rights of the masses just so they can conduct surveillance on the few then he should at least ask Congress for laws providing that authority instead of using the courts to force businesses into secretly becoming complicit in crimes against the American people."

On 2005, a U.S. Senator addressed a similar concern, when Congress was about to pass a law creating the "national security letter," a secret government process much more intense and unforgiving what Levison went through last summer:

> "This is legislation that puts our own Justice Department above the law. When national security letters are issued, they allow federal agents to conduct any search on any American, no matter how extensive, how wide-ranging, without ever going before a judge to prove that the search is necessary. All that is needed is a sign-off from a local FBI agent. That's it.
>
> "Once a business or a person receives notification that they will be searched, they are prohibited from telling anyone about it, and they're even prohibited from challenging this automatic gag order in court. Even though judges have already found that similar restrictions violate the First Amendment, this conference report disregards the case law and the right to challenge the gag order.
>
> "If you do decide to consult an attorney for legal advice, hold on. You will have to tell the FBI that you've done so. Think about that. You want to talk to a lawyer about whether or not your actions are going to be causing you to get into trouble. You've got to tell the FBI that you're consulting a lawyer. This is unheard of. There is no such requirement in any other area of the law. I see no reason why it's justified here.
>
> "And if someone wants to know why their own government has decided to go on a fishing expedition through every personal record or private document, through the library books that you read, the phone calls that you've made, the emails that you've sent, this legislation gives people no rights to appeal the

need for such a search in a court of law. No judge will hear your plea; no jury will hear your case. This is just plain wrong."

The question is: how much of a police state do we have already?

That Senator was concerned eight years ago, and that Senator was Barack Obama. Today, national security letters are part of the law of the land, the Obama administration uses them, and if you get one, talking about it is against the law. In that context, since Ladar Levison apparently did not get a national security letter, he was lucky. The country, not so much.

On October 10, in the United States Court of Appeals for the Fourth Circuit, Lavabit filed the opening brief of its appeal of the lower court's orders. The United States has until November 4 to file its answer. This will take awhile, it will take effort to follow, but it matters.

Note: Since the lifting of the federal court gag order on October 2, Ladar Levison and his company, Lavabit, have been getting some media attention (including a somewhat snide and incomplete story on page one of the New York Times). What follows in an effort to reconstruct at least the outline of a personal nightmare inflicted by our government on a small business owner who had done no wrong, even in the government's eyes – at least until he started taking his constitutional rights seriously.

Articles by: William Boardman