Volume 119 | Issue 3 Article 7

April 2017

Lavabitten

Brian L. Owsley
University of Norh Texas Dallas College of Law

LAVABITTEN

*Brian L. Owsley**

In 2013, at the height of the revelations about Edward Snowden and the National Security Administration's spying on American citizens even on American soil, a Texas company, Lavabit, and its founder Ladar Levison were making a name for themselves as Mr. Snowden's email provider.[1] Mr. Snowden had chosen Lavabit because its encryption was extremely effective at protecting the security of his emails.[2] When consumers learned that Lavabit was good enough for Mr. Snowden, some of them concluded that Lavabit was good enough for them, leading to a spike in the email provider's subscribers.[3]

[*] Brian L. Owsley, Assistant Professor of Law, University of North Texas Dallas College of Law; B.A., 1988, University of Notre Dame, J.D., 1993, Columbia University School of Law, M.I.A., 1994, Columbia University School of International and Public Affairs. From 2005 until 2013, the author served as a United States Magistrate Judge for the United States District Court for the Southern District of Texas.

[1] Kashmir Hill, *Email Company Used by Edward Snowden Shuts Down Rather Than Hand Data Over to Feds*, FORBES (Aug. 8, 2013, 3:45 PM), http://www.forbes.com/sites/kashmirhill/2013/08/08/email-company-reportedly-used-by-edward-snowden-shuts-down-rather-than-hand-data-over-to-feds/#751724107e0e.

[2] *Id.*

[3] Kashmir Hill, *Lavabit's Ladar Levison: "If You Knew What I Know About Email, You Might Not Use It,"* FORBES (Aug. 9, 2013, 5:35 PM), http://www.forbes.com/sites/kashmirhill/2013/08/09/lavabits-ladar-levison-if-you-knew-what-i-know-about-email-you-might-not-use-it/.

About four months after the FBI first approached Mr. Levison regarding its investigation into Mr. Snowden, he closed Lavabit.[4] Initially, the government applied for a pen register from a United States magistrate judge, who granted the order and enabled the government to collect real-time information about Mr. Snowden. The magistrate judge further ordered that Lavabit provide any necessary technical assistance to accomplish this task.[5] Subsequently, the government obtained a court order from the district judge requiring Lavabit to provide its passwords, encryption keys, and computer code.[6] Mr. Levison was willing to surrender the encrypted data related to Mr. Snowden's email account, as he had done several times in the past regarding criminal investigations, but he concluded that giving the government all of the requested information would put all of Lavabit's customers at risk.[7]

In the end, Mr. Levison closed Lavabit, and the government received none of the information it was seeking about Mr. Snowden.[8] The district court held Lavabit and Mr. Levison in contempt.[9] They both appealed to the United States Court of Appeals for the Fourth Circuit, which affirmed the district court.[10] In the end, punishing Lavabit and Mr. Levison essentially destroyed Lavabit because Mr. Levison decided that he could not protect Lavabit's subscribers in the manner he represented to them.[11] Consequently, he closed down Lavabit as an email provider.[12]

This Article addresses issues raised by the government's electronic surveillance requests of Lavabit that resulted in the closing of the company. Courts must safeguard individuals and companies from government overreach that will jeopardize their well-being. In Part I, I discuss at length the facts of the legal case involving the government's pen register application and the subsequent orders, as well as the response by Lavabit and Mr. Levison. Part II will unpack the legal analysis by the Fourth Circuit, discussing some of the pertinent issues raised by the appellate decision. In Part III, I address the recent dispute between Apple and the FBI as a comparison and contrast to the Lavabit

[4] Ladar Levison, *Secrets, Lies and Snowden's Email: Why I Was Forced to Shut Down Lavabit*, GUARDIAN: OPINION (May 20, 2014, 7:30 AM), https://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down-snowden-email.

[5] *In re* Under Seal, 749 F.3d 276, 280–81 (4th Cir. 2014).

[6] Nicole Perlroth & Scott Shane, *As F.B.I. Pursued Snowden, an E-Mail Service Stood Firm*, N.Y. TIMES (Oct. 2, 2013), http://www.nytimes.com/2013/10/03/us/snowdens-e-mail-provider-discusses-pressure-from-fbi-to-disclose-data.html.

[7] Hill, *supra* note 1; Perlroth & Shane, *supra* note 6.

[8] Levison, *supra* note 4.

[9] *Id.*

[10] *Id.*

[11] *Id.*

[12] *Id.*

case. Part IV will address the All Writs Act[13] and its applicability in these types of actions. Finally, Part V seeks to demonstrate the lessons to be learned from the San Bernardino shooting and Lavabit's troubles.

I. The Rise of Edward Snowden and the Fall of Lavabit

In order to understand the demise of Lavabit, one must recall Edward Snowden's release of classified National Security Agency documents.[14] Those revelations began on June 5, 2013.[15] Within the month, on June 28, 2013, a federal magistrate judge in the United States District Court for the Eastern District of Virginia signed an order authorizing the government to place a pen register[16] and a trap and trace device[17] on Lavabit's system.[18] Specifically, the government sought all metadata related to the email account of the target, Edward Snowden, but none of the contents of any of the emails.[19] In other words, the government was only authorized to obtain what has been analogously described as the external envelope information, including "the how, when, and where of the message."[20]

[13] 28 U.S.C. § 1651 (2012).

[14] *See generally* Perlroth & Shane, *supra* note 6.

[15] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013, 6:05 AM), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; *see also* Matthew Cole & Mike Brunker, *Edward Snowden: A Timeline*, NBC NEWS, (May 26, 2014, 5:43 PM), http://www.nbcnews.com/feature/edward-snowden-interview/edward-snowden-timeline-n114871.

[16] A pen register essentially records the outgoing dialed numbers from a given telephone number. 18 U.S.C. § 3127(3) (2012). It is defined as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication[.]" *Id.*

[17] A trap and trace device essentially records the incoming telephone numbers to a given telephone number. 18 U.S.C. § 3127(4) (2012). It is defined as:

> [A] device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication[.]

Id.

[18] *In re* Under Seal, 749 F.3d 276, 280–81 (4th Cir. 2014).

[19] *Id.* at 281.

[20] Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 384 (2014).

Shortly after the government obtained this court order, FBI agents met with Levison regarding the order.[21] Lavabit provided encrypted email service that was stored on its servers.[22] However, access to these encrypted emails was impossible without knowing a user's password because the messages were protected by a user's public key, while the corresponding private key necessary for decryption was secured by the user's password.[23] The FBI sought to compel the disclosure of the Lavabit TLS[24] key, which would allow it to intercept Snowden's password using a Man-in-the-Middle[25] attack.[26] With Snowden's password, the FBI could reverse the encryption process.[27]

According to the FBI, Lavabit either refused to comply or indicated that it was incapable of complying with the request because of Snowden's encryption.[28] According to Lavabit, it was willing to allow the pen register and trap and trace device to be installed on the system, but was uncomfortable in surrendering to the FBI Lavabit's encryption key because it would have allowed the FBI unfettered access to *all* of Lavabit's customers.[29]

After several days of discussions between Lavabit and the FBI, the government sought another court order.[30] Another magistrate judge issued an order compelling Lavabit comply with the original June 28, 2013 order.[31] On July 9, 2013, the government then sought a show cause order directing Lavabit and Levison to appear and explain why they had failed to comply with the June

[21] DEF CON Conference, *DEF CON 24—Ladar Levison—Compelled Decryption: State of the Art in Doctrinal Perversity*, YOUTUBE (Nov. 3, 2016), https://www.youtube.com/watch?v=JQiDGH2OW6k.

[22] *Id.*

[23] *Id.*

[24] TLS stands for "Transport Layer Security," which is a cryptographic protocol used to provide security on a computer network. *See* HOLLY LYNNE MCKINLEY, SSL AND TLS: A BEGINNER'S GUIDE 8 (2003), https://www.sans.org/reading-room/whitepapers/protocols/ssl-tls-beginners-guide-1029.

[25] A Man-in-the-Middle attack is a method of eavesdropping by which a third party inserts itself as a relay or proxy between the communications of two individuals, thus enabling the third party to receive information that was never intended to be provided to it. *Man in the Middle (MITM) Attack*, VERACODE, http://www.veracode.com/security/man-middle-attack (last visited Mar. 22, 2017).

[26] DEF CON Conference, *supra* note 21.

[27] *Id.*

[28] *In re* Under Seal, 749 F.3d 276, 281 (4th Cir. 2014).

[29] Ladar Levison, *Victimize / Terrorized*, SPRINGFIELDDOH, http://springfieldoh.ddns.net:47808/time%20warner/a%20necessary%20history.html (last visited Mar. 17, 2017).

[30] *See In re Under Seal*, 749 F.3d at 281.

[31] *See id.* at 280–81.

28 order.[32] In particular, the government accused Lavabit of stalling and ignoring the FBI's repeated attempts to resolve the matter.[33] Levison disputed the government's assertion: "The government lawyers tried to overwhelm me. In the first two weeks, I was served court orders a total of seven times leading to contact with the FBI every other day. (This was the stretch a prosecutor would later characterize as the 'long period of silence.')"[34]

On July 13, 2013, when it became clear that the order was seeking metadata, Lavabit offered to collect just the information itself and provide it to the FBI.[35] However, the government rejected this offer.[36] On July 16, 2013, the government obtained a seizure warrant requiring that Lavabit provide all information for decrypting Snowden's Lavabit emails, "including encryption keys and SSL keys."[37] This seizure warrant was not served on Levison.[38]

At a July 16 show cause hearing before the district court, appearing pro se, Levison testified that Lavabit had always agreed to comply with the installation of the pen register.[39] However, he objected to providing the government with Lavabit's encryption keys because that would eviscerate the system's overall security.[40] After this July 16 hearing, Lavabit did install the pen register, but much of the captured data was useless to the government because the encryption rendered it largely indecipherable.[41] Conversely, Levison indicated the login data was unusable, making it impossible to capture the password, but in all likelihood they did capture metadata, because email messages which contain metadata were not encrypted when traveling between servers much of the time.[42]

A second hearing was scheduled to assess Lavabit's compliance, but prior to that hearing, Levison and Lavabit filed a motion to quash the seizure warrant.[43] Specifically, they asserted "that the warrant (1) amounted to an impermissible general warrant barred by the Fourth Amendment; (2) sought immaterial information; and (3) imposed an undue burden on Lavabit's business."[44] On August 1, 2013, the district court conducted a second hearing

[32] *See id.* at 281–82.

[33] *See id.*

[34] Levison, *supra* note 29.

[35] *See In re Under Seal*, 749 F.3d at 282.

[36] *Id.*

[37] *Id.* at 282–83.

[38] *See id.* at 283.

[39] *See id.*

[40] *See id.*

[41] *See id.*

[42] Levison, *supra* note 29.

[43] *See In re Under Seal*, 749 F.3d at 283.

[44] *Id.*

where it determined "that the Government would not collect all users' data, even if the encryption keys would practically enable the Government to access all that data."[45]

After the August 1 hearing, Senior United States District Judge Claude Hilton issued an order requiring Lavabit to provide the encryption keys to the government as well as any necessary assistance to accomplish the goals of the pen register order.[46] Lavabit responded by "provid[ing] the FBI with an 11-page printout containing largely illegible characters in 4-point type."[47] When Lavabit refused to provide the key in electronic form, the government sought and received sanctions of $5000 per day for non-compliance on August 5, 2013.[48] Consequently, on August 7, 2013, Lavabit provided the FBI with the encryption keys.[49] Simultaneous to relinquishing the keys, Levison shut down Lavabit because he felt that to do otherwise would violate his conscience:

> 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.[50]

Ultimately, the government was unable to intercept Snowden's password and recover the encrypted messages stored on the Lavabit servers.[51]

II. THE FOURTH CIRCUIT REJECTS LAVABIT'S APPEAL OF THE CIVIL CONTEMPT ORDER

In response to the civil contempt order issued by Senior Judge Hilton, Lavabit filed an appeal of the civil contempt order, seeking a decision extricating

[45] *Id.* at 284.

[46] *See id.*

[47] *Id.*

[48] *See id.*

[49] *See id.*

[50] Levison, *supra* note 29; *see also In re Under Seal*, 749 F.3d at 284 n.11.

[51] Kim Zetter, *Encrypted Email Service Once Used by Edward Snowden Edward Snowden Relaunches*, INTERCEPT (Jan. 20, 2017, 12:57 PM), https://theintercept.com/2017/01/20/encrypted-email-service-once-used-by-edward-snowden-to-relaunch/.

it from the legal consequences of the order.[52] Ultimately, the United States Court of Appeals for the Fourth Circuit affirmed the civil contempt order finding that Lavabit had not properly preserved its claims for appeal or waived them.[53] In arguing his position against providing the government with Lavabit's encryption keys, Levison said "I have only ever objected to turning over the SSL keys because that would compromise all of the secure communications in and out of my network, including my own administrative traffic."[54] The Fourth Circuit found this statement too vague and tenuous to form a legal issue before the court. In order to preserve an issue for appeal, a litigant must be specific so as to put the district court on notice that a party was challenging the matter.[55] Here, the court concluded that "[n]either the district court nor the Government therefore had any signal from Lavabit that it contested the district court's authority under the Pen/Trap Statute to enter the Pen/Trap Order or the June 28th Order."[56]

Next, Lavabit argued that it was induced or invited to waive its appeal regarding the encryption keys by the district court and the government.[57] However, the Fourth Circuit concluded that Lavabit was aware that the June 28 order concerned encryption keys and thus could not have been induced or invited to waive the issue.[58] Ultimately, the court held that Lavabit abandoned any argument that it did not raise before the trial court and cannot raise anew on appeal.[59]

Levison maintains that some of the difficulty that Lavabit faced was his inability to hire counsel that understood both the law and the technology involved:

> Because the whole case was under seal, I couldn't admit to anyone who wasn't a lawyer that I needed help, let alone why. In the days before my appearance I would spend hours repeating the facts of the case to a dozen attorneys, as I sought someone else that was qualified to represent me.[60]

Indeed, he appeared at his first hearing pro se because his first attorney was unable to attend.[61] Even when he was able to retain counsel, there were several difficult issues:

[52] *See In re Under Seal*, 749 F.3d at 284.

[53] *See id.* at 288.

[54] *Id.* at 287.

[55] *See id.* at 287–88.

[56] *Id.* at 288.

[57] *See id.*

[58] *See id.* at 288–89.

[59] *See id.* at 292–93.

[60] Levison, *supra* note 29.

[61] *In re Under Seal*, 749 F.3d at 283.

> I retained a small local law firm before returning home, and they took on the task of assembling a legal strategy and filing briefs in the few short days available. The court barred them from consulting outside experts, making it difficult to understand the complex legal and technological issues involved. Even a request to discuss the case with members of Congress was denied. To make matters worse, the court wouldn't deliver transcripts for my first appearance for another two months. My legal team was forced to proceed without access to information they needed.[62]

Finally, Judge Hilton found Levison in civil contempt at an ex parte proceeding.[63]

III. THE DISPUTE BETWEEN APPLE AND THE FBI INITIALLY RAISES CONCERNS SIMILAR TO ISSUES FACED BY LAVABIT

In order to better understand the Lavabit case, it is important to understand what the government did and did not use in pursuing the information that it sought from Lavabit. Specifically, the government based its legal authority to obtain the encryption keys on three sources:[64] a grand jury subpoena, which was subsequently withdrawn;[65] the language regarding technical assistance in the pen register and trap and trace statutes;[66] and the Stored Communications Act.[67] Arguments regarding the latter two bases were waived. The Fourth Circuit notes that there are differences between the pen register statute and the trap and trace statute insofar as the latter requires technical assistance in both the installation and the operation of the device whereas the former requires technical assistance in just the installation.[68]

Notably absent from the government's arsenal in the Lavabit case was the All Writs Act, which Congress enacted in 1789, authorizing "[t]he Supreme Court and all courts established by Act of Congress [to] issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."[69] The All Writs Act played a central role in a more recent case involving the government's electronic surveillance and demands for third-party assistance: the dispute between Apple and the FBI.

In December 2015, Syed Rizwan Farook and his wife Tashfeen Malik participated in a mass shooting at his workplace in San Bernardino, California,

[62] Levison, *supra* note 29.

[63] *See id.*; *see also In re Under Seal*, 749 F.3d at 284.

[64] Levison, *supra* note 29.

[65] *See In re Under Seal*, 749 F.3d at 289.

[66] 18 U.S.C. § 3124 (2012).

[67] *See generally* 18 U.S.C. §§ 2701–12 (2012).

[68] *See In re Under Seal*, 749 F.3d at 291–92.

[69] 28 U.S.C. § 1651(a) (2012).

killing 14 people.[70] This attack would no doubt have garnered significant attention by the FBI, but because Malik declared her allegiance to ISIS prior to her death in the attack,[71] the FBI's scrutiny was heightened.

When he died, Farook had an iPhone 5c running iOS Version 9 Operating System, which the FBI wanted to access.[72] His employer, the San Bernardino County Public Health Department, provided him with this cell phone and also authorized the FBI to access it during the course of its investigation.[73] Unfortunately, Farook had previously set his iPhone so that one needed a four-digit password to access it.[74] Moreover, attempting to randomly enter numbers to ascertain the correct password could cause the iPhone to erase all its data once agents had reached a preset number of failed password attempts.[75]

In February 2016, the FBI requested for Apple to help it accessing Farook's iPhone and thus his data.[76] However, Apple did not cooperate in a manner that satisfied the FBI, so it obtained a federal court order requiring Apple to assist the FBI in accessing Farook's cell phone.[77]

Apple and the FBI also waged a war of words promoting their positions in the legal battle. Tim Cook, Apple CEO, published an open letter to its customers condemning the FBI's tactics as a "dangerous precedent":

> We have great respect for the professionals at the FBI, and we believe their intentions are good. Up to this point, we have done everything that is both within our power and within the law to help them. But now the U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create. They have asked us to build a backdoor

[70] Adam Nagourney, Ian Lovett & Richard Perez-Pena, *San Bernardino Shooting Kills at Least 14; Two Suspects Are Dead*, N.Y. TIMES (Dec. 2, 2015), http://www.nytimes.com/2015/12/03/us/san-bernardino-shooting.html?_r=0; Pat St. Claire, Greg Botelho & Ralph Ellis, *San Bernardino Shooter Tashfeen Malik: Who Was She?*, CNN (Dec. 8, 2015), http://www.cnn.com/2015/12/06/us/san-bernardino-shooter-tashfeen-malik/.

[71] Claire, Botelho & Ellis, *supra* note 70.

[72] Joel Rubin, James Queally & Paresh Dave, *FBI Unlocks San Bernardino Shooter's iPhone and Ends Legal Battle with Apple, for Now*, L.A. TIMES (Mar. 28, 2016, 10:39 PM), http://www.latimes.com/local/lanow/la-me-ln-fbi-drops-fight-to-force-apple-to-unlock-san-bernardino-terrorist-iphone-20160328-story.html.

[73] Atoosa Moinzadeh, *FBI Approved Hack that Complicated Access to San Bernardino Shooter's iPhone Data*, VICE NEWS (Feb. 21, 2016, 3:35 PM), https://news.vice.com/article/fbi-approved-hack-that-complicated-access-to-san-bernardino-shooters-iphone-data.

[74] Rubin, Queally & Dave, *supra* note 72.

[75] Moinzadeh, *supra* note 73.

[76] *Id.*

[77] *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No. ED 15-0451M, 2016 WL 618401, at *1 (C.D. Cal. Feb. 16, 2016) (issuing an order compelling Apple, Inc. to assist agents in search).

> to the iPhone.
>
> Specifically, the FBI wants us to make a new version of the iPhone operating system, circumventing several important security features, and install it on an iPhone recovered during the investigation. In the wrong hands, this software—which does not exist today—would have the potential to unlock any iPhone in someone's physical possession.
>
> The FBI may use different words to describe this tool, but make no mistake: Building a version of iOS that bypasses security in this way would undeniably create a backdoor. And while the government may argue that its use would be limited to this case, there is no way to guarantee such control.[78]

Not to be outdone, James Comey, the FBI Director, issued a responsive press release asserting that the FBI's assistance request was necessary:

> The particular legal issue is actually quite narrow. The relief we seek is limited and its value increasingly obsolete because the technology continues to evolve. We simply want the chance, with a search warrant, to try to guess the terrorist's passcode without the phone essentially self-destructing and without it taking a decade to guess correctly. That's it. We don't want to break anyone's encryption or set a master key loose on the land. I hope thoughtful people will take the time to understand that. Maybe the phone holds the clue to finding more terrorists. Maybe it doesn't. But we can't look the survivors in the eye, or ourselves in the mirror, if we don't follow this lead.
>
> ***
>
> So I hope folks will remember what terrorists did to innocent Americans at a San Bernardino office gathering and why the FBI simply must do all we can under the law to investigate that. And in that sober spirit, I also hope all Americans will participate in the long conversation we must have about how to both embrace the technology we love and get the safety we need.[79]

These two statements set up a public debate between a large American technology company and the chief federal law enforcement agency.

[78] Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), http://www.apple.com/customer-letter/.

[79] James Comey, *FBI Director Comments on San Bernardino Matter*, FBI (Feb. 21, 2016), https://www.fbi.gov/news/pressrel/press-releases/fbi-director-comments-on-san-bernardino-matter.

Then as quickly as it began, it was more or less over. On March 28, 2016, the FBI informed the district court Apple's assistance was no longer necessary because it had "successfully accessed the data stored on Farook's iPhone."[80] Apparently, the FBI had been able to breach Apple's security system for Farook's iPhone with the assistance of a hacker who was paid at least $1.3 million for the work.[81]

IV. THE FBI SOUGHT TO USE THE ALL WRITS ACT IN ITS DISPUTE WITH APPLE

If the hacker had been unsuccessful, then the FBI would have continued with its argument that the All Writs Act authorized the district court to require Apple to assist the FBI.[82] However, according to the Supreme Court, the Act provides for an extraordinary writ that should be used only in an extraordinary circumstance.[83] The Court has further explained in analyzing this writ that while the "Act empowers federal courts to fashion extraordinary remedies when the need arises, it does not authorize them to issue ad hoc writs whenever compliance with statutory procedures appears inconvenient or less appropriate."[84]

In *United States v. New York Telephone Company*,[85] the Supreme Court analyzed the All Writs Act, and found that a district court could require a telephone company to provide the government telephone numbers pursuant to a pen register based on the writ.[86] In focusing on whether the All Writs Act can be used in conjunction with a pen register, the Court determined "that the power of federal courts to impose duties upon third parties is not without limits [as] unreasonable burdens may not be imposed."[87]

In the FBI's dispute with Apple regarding assistance decrypting Farook's iPhone, the government expected Apple's cooperation, in part, because it had received assistance with other Apple devices. By one account, Apple had

[80] Katie Benner & Eric Lichtblau, *U.S. Says It Has Unlocked iPhone Without Apple*, N.Y. TIMES (Mar. 28, 2016), http://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html?_r=0.

[81] *Id.*; Julia Edwards, *FBI Paid More than $1.3 Million to Break into San Bernardino iPhone*, REUTERS (Apr. 22, 2016, 1:47 PM), http://www.reuters.com/article/us-apple-encryption-fbi-idUSKCN0XI2IB.

[82] *See* Benner & Lichtblau, *supra* note 80.

[83] Platt v. Minn. Min. & Mfg. Co., 376 U.S. 240, 245 (1964) (quoting *Ex parte* Fahey, 332 U.S. 258, 260 (1947)).

[84] Pa. Bureau of Corr. v. U.S. Marshals Serv., 474 U.S. 34, 43 (1985).

[85] 434 U.S. 159, 176 (1977).

[86] *See id.* at 174–76.

[87] *Id.* at 172.

assisted the government in accessing iPhones on at least 70 occasions.[88] A few recent federal orders by federal magistrate judges support the contention that Apple had been more cooperative regarding assisting federal law enforcement.[89] In filing these applications, Assistant United States Attorneys would represent to the courts that other courts have granted similar orders and Apple has complied: "The government is aware, and can represent, that in other cases, courts have ordered the unlocking of an iPhone under this authority [i.e., the All Writs Act]. Additionally, Apple has routinely complied with such orders."[90] However, these California cases simply mandated "that Apple shall provide *reasonable technical assistance* to enable law enforcement agents to obtain access to unencrypted data ("Data") on the Device."[91] More important, the courts "further ordered that, to the extent that data on the iOS device is encrypted, Apple may provide a copy of the encrypted data to law enforcement but Apple is not required to attempt to decrypt, or otherwise enable law enforcement's attempts to access any encrypted data."[92] In other words, the approach that the FBI took in the case of Farook's iPhone was not the same as that in previous cases. Instead, the FBI was demanding more than "reasonable technical assistance" in providing unencrypted data in seeking to compel Apple to decrypt Farook's iPhone.

The FBI's demands on Apple regarding the San Bernardino case were problematic not only because of the new approach, but because it would likely have violated the All Writs Act. The Supreme Court, in discussing the All Writs Act, has explained that "the power of federal courts to impose duties upon third

[88] Evan Perez, *DOJ: Apple Has Routinely Helped Law Enforcement—Until Recent Publicity*, CNN (Feb. 23, 2016, 10:57 AM), http://www.cnn.com/2016/02/23/politics/apple-justice-department/.

[89] *In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, No. 5:14-CR-90470 (N.D. Cal. June 6, 2014) (order requiring Apple to assist agents in Apple iOS device search); *In re* Order Requiring [XXX], Inc. to Assist in the Execution of a Search Warrant Issued by this Court by Unlocking a Cellphone, No. 14 Mag. 2258, 2014 WL 5510865 (S.D.N.Y. Oct. 31, 2014); *In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, No. 4:14-CR-90812 (N.D. Cal. Nov. 3, 2014) (order requiring Apple to assist agents in iPhone search).

[90] *In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, No. 4:14-CR-90812 (N.D. Cal. Nov. 3, 2014) (application order requiring Apple to assist agents in iPhone search).

[91] *In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, No. 5:14-CR-90470 (N.D. Cal. June 6, 2014) (order requiring Apple to assist agents in Apple iOS device search) (emphasis added); *accord In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, No. 4:14-CR-90812 (N.D. Cal. Nov. 3, 2014) (order requiring Apple to assist agents in iPhone search).

[92] *In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, No. 4:14-CR-90812 (N.D. Cal. Nov. 3, 2014) (order requiring Apple to assist agents in iPhone search); *accord In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, No. 5:14-CR-90470 (N.D. Cal. June 6, 2014) (order requiring Apple to assist agents in Apple iOS device search).

parties is not without limits."[93] Specifically, the Court determined that any order pursuant to the All Writs Act cannot inflict "[u]nreasonable burdens" on the third party.[94] If the dispute between the FBI and Apple regarding Farook's iPhone had proceeded, Apple likely would have argued that the FBI's request was unreasonably burdensome in that it was not able to readily decrypt the sophisticated level of operating software that the phone was using. Moreover, even if it could decrypt it, that endeavor would take countless employee hours and costs as well as destroy Apple's security for its operating software. Such consequences must be acknowledged as too burdensome.

In a case similar to Apple's dispute and analogous to Lavabit's circumstances, the government sought a court order mandating that Apple assist DEA agents to bypass the security regarding the iPhone user's password.[95] In analyzing the government's application, a federal magistrate first notes that the statute has three requirements for an order compelling Apple to circumvent its security to provide the DEA with the iPhone's password:

> (1) issuance of the writ must be "in aid of" the issuing court's jurisdiction;
> (2) the type of writ requested must be "necessary or appropriate" to provide such aid to the issuing court's jurisdiction; and
> (3) the issuance of the writ must be "agreeable to the usages and principles of law."[96]

If the government's application meets all three of these requirements, then the presiding judge *may* exercise the discretion to grant the application, but is not required to do so.[97]

In discussing the first requirement, the magistrate judge determined that an order compelling Apple to circumvent its security to provide the DEA with the iPhone's password would aid in the court's jurisdiction.[98] Moreover, he concluded that this type of order was necessary or appropriate in aiding the

[93] United States v. N.Y. Tel. Co., 434 U.S. 159, 172 (1977); *accord In re* Order Requiring [XXX], Inc. to Assist in the Execution of a Search Warrant Issued by this Court by Unlocking a Cellphone, 2014 WL 5510865, at *2 (S.D.N.Y Oct. 31, 2014).

[94] *N.Y. Tel. Co.*, 434 U.S. at 172; *accord In re* Order Requiring [XXX], Inc. to Assist in the Execution of a Search Warrant Issued by this Court by Unlocking a Cellphone, 2014 WL 5510865, at *2 (S.D.N.Y Oct. 31, 2014).

[95] *In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, 149 F. Supp. 3d 341 (E.D.N.Y. 2016).

[96] *Id.* at 350.

[97] *See id.* at 351; *see also N.Y. Tel. Co.*, 434 U.S. at 176–77.

[98] *See In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, 149 F. Supp. 3d at 351–52.

court's jurisdiction.[99] However, the judge ultimately found that such an order would not be "agreeable to the usages and principles of law."[100] In the end, the magistrate judge denied a similar type of request that would have been less intrusive than the one sought in the San Bernardino case.

V. HOW DO LAVABIT AND THE APPLE DISPUTE OVER THE SAN BERNARDINO SHOOTING RELATE TO EACH OTHER?

Why does all of this matter to Lavabit? On some level, it doesn't. Lavabit's secured email services have been shuttered for over three years. The damage has been done and is likely permanent.

On the other hand, it is important to understand the similarities and differences between the circumstances surrounding Lavabit and the situation for Apple. Lavabit was a relatively small operation serving at most a little over 400,000 subscribers. Apple is a large multinational corporation that may be the technology equivalent of too big to fail. Lavabit was too small to fight back in any meaningful way when the government came calling.

In many ways, Lavabit would have theoretically been better off if the government had sought to compel Lavabit's assistance in decrypting Snowden's password pursuant to the All Writs Act. In such a case, Lavabit would have been entitled to a hearing. Indeed, because the Fourth Circuit affirmed the civil contempt order finding that Lavabit had essentially waived all challenges to it, there was unfortunately no resolution to the underlying legal questions about the basis for requiring Lavabit to assist the government.

More important, if the standard applied by the court concerned the burdensomeness that Lavabit would experience in handing over its encryption keys to government, then the outcome would likely be different. As several cases concerning the All Writs Act established, orders requiring a provider to assist in access to unencrypted data are permissible while mandating assistance to decrypt is generally not permissible.[101] In the end, Lavabit and other smaller providers like it are vulnerable to the government in a way that Apple might not be, which can defend itself should the government continue to rely on the All Writs Act.

VI. CONCLUSION

In the heat of the moment, the government went after Lavabit with everything that it could bring to bear on the company. Indeed, it convinced the courts that Lavabit was acting in contempt. No doubt, the government was desperate to obtain information about Snowden and use that information to capture him. In hindsight, all of those efforts failed. In the end, Snowden moved

[99] *Id.* at 352.

[100] *Id.* at 362–63.

[101] *See supra* Part IV.

from Hong Kong to Russia where he still lives today avoiding extradition to the United States[102] and potentially cooperating with his Russian handlers.

On the other hand, Lavabit closed for over three years, losing significant revenue.[103] Moreover, in its closing the government missed its opportunity to obtain the information that it sought originally. The government insisted that Lavabit fully cooperate on its own terms instead of working with Lavabit and Mr. Levison to get the information that it sought. If the government cannot change its approach, they will lose valuable information from the next Lavabit or from larger corporations like Apple.

[102] *See* Jane Onyanga-Omara & Gregory Korte, *Edward Snowden's Residence Permit in Russia Extended by a "Couple of Years"*, USA TODAY (Jan. 18, 2017, 6:22 AM), www.usatoday.com/story/news/world/2017/01/18/russia-extends-edward-snowdens-residence-permit/96709018/.

[103] LAVABIT, https://lavabit.com/ (last visited Apr. 22, 2017).