No. 13-4635(L); 13-4626

IN THE UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

UNDER SEAL,

Party-in-Interest-Appellant.

On Appeal from the United States District Court
For the Eastern District of Virginia

REPLY BRIEF OF APPELLANT

Jesse R. Binnall
BRONLEY & BINNALL, PLLC
10387 Main Street
Suite 201
Fairfax, VA 22030
703.229.0335

Ian Samuel
JONES DAY
222 E. 41st Street
New York, NY
212.326.3808

Marcia Hoffman
LAW OFFICE OF MARCIA HOFFMAN
25 Taylor Street
San Francisco, CA 94102
415.830.6664

David Warrington
Laurin Mills
LECLAIRRYAN
2318 Mill Road
Suite 1100
Alexandria, VA 22314
703.647.5926

Counsel for Party in Interest-Appellant

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

OTHER AUTHORITIES

INTRODUCTION

The government has no general entitlement to enlist innocent third parties in its surveillance efforts; it may do so only to the extent that the law explicitly provides. In this case, neither the pen-trap order nor the Stored Communications Act warrant validly allowed the government to seize Lavabit's private encryption keys.[1] The pen register statute does not authorize the government to demand that sort of assistance; a service provider only must help the government ensure that its pen-trap device is installed and operated "unobtrusively and with a minimum of interference with the services" provided. 18 U.S.C. §3124(a), (b). And the warrant was riddled with flaws: (1) it sought information that does not pertain to a subscriber; (2) it imposed an undue burden on the company; (3) it did not have as its object the fruits, instrumentalities, or evidence of crime; and (4) it permitted general rummaging through all of Lavabit's customer communications.

In response, the government dedicates a huge proportion of its brief to arguing that Lavabit's objections to the orders were waived. They were not. Proceeding *pro se*, Mr. Levison nonetheless objected—in person, and in district court—to the pen-trap order. In response, the government begged off, insisting that its warrant meant the parties could "avoid litigating the issue." See App. 43. And Lavabit objected to the warrant by written motion. See App. 66-73. "Once a federal claim is properly

[1] The opening brief also argued that the grand jury subpoena was invalid. We accept the government's concession (at 13) that it is not relying on the subpoena to justify the seizure of Lavabit's encryption keys; this point was pressed in the opening brief only to ensure full adversarial presentation of all possible issues.

presented, a party can make any argument in support of that claim"—that simple and flexible rule suffices to reject all of the government's waiver arguments. *Yee v. Escondido*, 503 U.S. 519, 534 (1992).

I. The Pen Trap Order is invalid

A. Lavabit did not waive its objection to the pen-trap order

The government argues that Lavabit did not object below to the pen-trap order, and that this alleged waiver prevents this Court from considering our arguments about the order's propriety. Gov't Br. 13–19. The record demonstrates otherwise. During its very first appearance in district court, Lavabit objected to providing its encryption keys pursuant to the pen-trap order, despite the fact that Mr. Levison was proceeding *pro se* at that point. The government then responded that the pen-trap point was irrelevant, because it had secured a search warrant, and further proceedings were conducted accordingly. Under the circumstances, it is hardly fair to blame *Lavabit* for the fact that the pen-trap order's legality was not more thoroughly vetted in district court.

The basic rule of claim-preservation in federal courts is simple and flexible: "Once a federal claim is properly presented, a party can make any argument in support of that claim." *Yee*, 503 U.S. at 534. In other words, once a claim is fairly presented to the district court, "parties are not limited to the precise arguments they made below." *Ibid.* There are obvious limits to this principle—a due process claim may not be converted into an Eighth Amendment claim, for example, simply by

labeling both as claims of "unconstitutionality." See *Browning-Ferris Indus. of Vt., Inc. v. Kelco Disposal, Inc.*, 492 U.S. 257, 277 n.23 (1989). But Lavabit is not close to that line: it objected below to providing its encryption keys pursuant to the pen-trap order, just as it has here.

Given the government's exhaustive focus on waiver, it is necessary to review the proceedings below in some detail. Lavabit's owner, Mr. Levison, personally appeared before Judge Hilton on July 16, 2013. App. 39. The government began its presentation by asking the district court to inquire whether Mr. Levison was going to provide "the FBI with the encryption keys … called for by the pen register order." App. 39. Mr. Levison (though appearing a thousand miles from home, and *pro se*) took that as his cue, and requested "a couple of things by motion." App. 40. As relevant here, he stated that he had "always agreed to the installation of the pen register device," but objected to "turning over the [encryption] keys because that would compromise all the secure communications in and out of my network." App. 42.

Judge Hilton then expressed some uncertainty about whether the pen-trap order he had entered required Lavabit to turn over encryption keys at all. App. 43 ("My initial order ordered nothing but that the pen register be put in place."). The government disputed Judge Hilton's characterization of his order, but also said—crucially, for present purposes—that "*to avoid litigating this issue*, we asked the court to enter" the search warrant pursuant to the Stored Communications Act. App. 43 (emphasis added). Judge Hilton reiterated his understanding of his pen-trap order as

not requiring Lavabit to provide encryption keys, and the government again emphasized that the Stored Communications Act warrant nonetheless required those keys to be turned over. App. 43-44. Indeed, when Judge Hilton stated that he did not think he needed to reach the pen-trap issue because "I've issued a search warrant" for the encryption keys, the government responded: "Correct." App. 43. Judge Hilton then made clear that issues regarding the warrant and the grand jury subpoena needed to be litigated separately, see App. 47-48, and continued the proceedings until July 26th, App. 51-52.

It was the government's frank admission that it had secured the search warrant to "avoid litigating" the issue of the pen-trap order's legality, combined with Judge Hilton's perfectly plain statements that he did not understand his pen-trap order to require the encryption keys to be turned over, that led Lavabit to focus on the remaining areas of disagreement: the search warrant and the grand-jury subpoena. See App. 66-73. The August 1 hearing tracked these issues: When Judge Hilton asked the government what the issue before him was, and the government responded that it wanted him to "order the production of the encryption keys," a colloquy ensued that never once mentioned the pen-trap order. App. 114-117. After Lavabit provided the encryption keys in non-electronic format, the government moved, *ex parte*, for sanctions. App. 120-131. That motion—and the proposed order granting sanctions, see App. 132-133, which the district court granted without any opportunity for Lavabit to respond—mentioned the pen-trap order only in the most oblique fashion.

Given this course of events, it would have been fair for Lavabit to focus exclusively on the search warrant in this appeal. That was the issue to which the parties had winnowed the case below. But, out of an abundance of caution and to ensure full adversarial presentation of all issues that this Court might elect to reach, Lavabit's opening brief on appeal nonetheless set forth a case that the pen-trap order was invalid, just as it argued for the impropriety of the now-withdrawn grand-jury subpoena. But that does not change the fact that it was *the government* that told Lavabit and the district court that the search warrant's existence allowed the parties to "avoid litigating" the pen-trap question.

The government, of course, is perfectly aware of all of this. Litigation is not "a game, like golf, with arbitrary rules to test the skill of the players"; rather, the waiver and forfeiture doctrines exist to facilitate the "'winnowing process,'" such that courts know "what remains to be decided." *Poliquin v. Garden Way, Inc.*, 989 F.2d 527, 531 (1st Cir. 1993) (Boudin, J.). The government told the district court that what remained to be decided was the propriety of its search warrant. If arguments on other matters have been waived, they have surely not been waived by Lavabit.

At any rate, even if Lavabit had not made its objection to the pen-trap order below, there are many reasons that this Court should exercise its discretion to entertain Lavabit's arguments nonetheless. See *Exxon Shipping Co. v. Baker*, 554 U.S. 471, 487 (2008) (when to entertain an argument not presented below is "a matter left primarily to the discretion of the courts of appeals"). Mr. Levison was proceeding *pro*

se at the critical stage below, when the issue of the pen register's legality was first broached; "the long-standing practice is to construe *pro se* pleadings liberally." *Hill v. Braxton*, 277 F.3d 701, 707 (4th Cir. 2002). Indeed, as the initial hearing demonstrates, the government resisted efforts by Lavabit to secure counsel at an earlier date. Moreover, the legality of the pen-trap order presents a "pure question of law," such that the judicial system has an interest in resolving it without "further delay." *Council of Alternative Political Parties v. Hooks*, 179 F.3d 64, 69 (3d Cir. 1999); see also *Dean Witter Reynolds, Inc. v. Fernandez*, 741 F.2d 355, 360-61 (11th Cir. 1984) (same). Finally, the questions presented in this case are of immense public concern, as the media attention on this litigation amply demonstrates. See *Ex parte Republic of Peru*, 318 U.S. 578, 585 (1943) (whether to exercise discretionary judicial power properly informed by whether "a question of public importance is involved").

B. The Pen-Trap Order Commanded More Assistance Than the Statute Authorizes

The pen register statute does not require service providers to turn over their private encryption keys. Rather, the only assistance the statute requires is that which is necessary for the surveillance device to be installed and operated "unobtrusively and with a minimum of interference with the services" that the provider offers to the target of the investigation. See 18 U.S.C. §3124(a), (b) (identical language). Lavabit's encryption keys are not required to install or use the government's device unobtrusively, and thus Lavabit was not required by statute to provide them.

In response, the government first argues (at 23–24) that the statute contains two different standards for what assistance a service provider must give, depending on whether what is being installed is a "pen register" device, or a "trap and trace" device. It is quite strange for the government to suggest this, because (as it notes) its device was *both* a pen register *and* a trap-and-trace device. See Gov't Br. 22. But the government's statutory argument is worse than strange; it is wrong. The two standards, set forth in 18 U.S.C. §3124(a)–(b), are identical in the relevant respect. For a pen register, a service provider must furnish

> information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place…

18 U.S.C. §3124(a). For a trap-and-trace device, a service provider must furnish

> information, facilities and technical assistance including installation and operation of the device unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place…

18 U.S.C. §3124(b). The only difference is that a service provider need not assist in the operation of a pen register, but in both cases, the only assistance required is ensuring that the "installation" *or* "operation of the device" is done—as both sections recite, in identical terms—"unobtrusively and with a minimum of interference with the services" afforded to the target of the investigation. §3124(a), (b). See also Gov't

Br. 22 (quoting the relevant language of §3124(b) and italicizing all but the crucial adverb phrase).

Therefore, the government's argument (at 24) that Lavabit's encryption keys were necessary for the device to "function effectively" is both a *non sequitur* and untrue. It is a *non sequitur*, because what the statute requires providers to do is ensure that the device operates *unobtrusively*, not "effectively." And it is untrue because the device was installed and worked as designed without the encryption keys: it recorded all of the information coming in and out of Lavabit's servers. It just so happened that the communications that the government captured were encrypted. That does not mean that the device was not installed, or that it did not work; it still recorded the network addresses from which communications were sent, for example. All it means is that the government's surveillance turned up less than it was hoping for.

Nonetheless, the drafters of the pen-register statute chose not to require service providers to do everything in their power to guarantee that the government gets its man. The statute imposes only the more modest burden on providers of giving that aid necessary for the device to operate "unobtrusively and with a minimum of interference with the services" offered. No more. So while the FBI has candidly complained to Congress of a "gap between our legal authority to intercept electronic communications pursuant to court order and our practical ability to actually intercept those communications," it is not permitted to close that perceived "gap" by ordering service providers to do more than the statute contemplates. Valerie Caproni (FBI

General Counsel), *Statement Before the House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security* (Feb. 17, 2011), available at http://www.fbi.gov/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies.

Finally, the government argues (at 25–26) that the encryption keys *were* necessary to install the pen register—in other words, that the pen register was not "installed" (despite being attached to the target servers, turned on, and capturing data) until Lavabit turned over information needed to decode some of the intercepted information. That is a truly unnatural sense of the word "installed"—for one thing, the statutory text refers disjunctively to "installation" and "operation," see 18 U.S.C. §3124(b). For another, the government's dictionary definitions of "install"—which are all slight variations on "to set in position and connect or adjust for use"—illustrate the opposite point. The government's device *was* placed "in position" and "connected" for use, and it was capturing data just as it was designed to, some of which was encrypted. The government's novel reimagining of the word "installed" is so avant-garde that not even the government can remember to stick to it; observe:

1. "Prior to the August 1 hearing, and after discussions with Mr. Levison, *the FBI installed a pen/trap device* to capture the information sought by the pen/trap order." Gov't Br. 8 (correctly acknowledging the device was "installed" prior to the keys being turned over on August 7) (emphasis added).
2. "Mr. Levison did not indicate whether he would allow the FBI to install the pen/trap device *or* provide the encryption keys." Gov't Br. 5 (correctly

describing installation of the device and provision of the keys as two different actions) (emphasis added). (As noted above, Mr. Levison did not object to the installation of the device itself. See App. 42.)

3. "On a later date, and after discussions with Mr. Levison, *the FBI installed a pen-trap device* on Lavabit's Internet service provider, which would capture the same information as if a pen-trap device were installed on Lavabit's server." Response of the United States in Opposition to Lavabit's Motion to Quash, App. 85 (correctly acknowledging that installation had occurred before the encryption keys were turned over).[2]

The government had it right the first few times.

Finally, nothing about this argument permits a service provider to lock its doors and prevent the government from installing its device, as the government suggests (at 27). A provider must aid unobtrusive installation—but need not help with effective investigation. The government's argument would render service providers little more than its junior surveillance adjuncts; under its view of the statute, the government could presumably even order service providers to "assist" it by modifying their systems to aid its surveillance, despite the explicit decision of Congress to exempt businesses like Lavabit from the provider-assistance provisions of CALEA. See 47 U.S.C. §1002; compare Gov't Br. 29 n.9 (suggesting that Congress' exclusion of businesses like Lavabit from CALEA is essentially without effect).

[2] The government's "on a later date" circumlocution is typical. Despite its detailed timeline of every other event, the government has never specified the actual date that it installed the pen-trap device. It is clear from these sentences that it was prior to Lavabit turning over its encryption keys, but just how much sooner is unclear—the government may have even installed it prior to Lavabit's first appearance in court.

II. The Stored Communications Act Warrant Was Invalid

In the opening brief, Lavabit pointed to four independent defects in the government's Stored Communications Act warrant: (1) it did not seek the "contents of a wire or electronic communication" or "information pertaining to a subscriber," which is all the statute permits; (2) it caused an undue burden on Lavabit, which the statute forbids; (3) it did not seek the fruits, evidence, or instrumentalities of a crime, which the Fourth Amendment requires; and (4) it permits general rummaging through other subscribers' communications, which the Fourth Amendment forbids.

Any one of these arguments is enough to defeat the warrant's validity. To succeed, the government must run the table and to win every statutory and Constitutional argument about the warrant. Conversely, if this Court concludes that one of Lavabit's arguments is correct, there is no need to reach any of the others.

A. The warrant does not pertain to a subscriber

The simplest reason to hold the warrant invalid is that it does not seek information about a subscriber; the encryption keys are information pertaining, at most, to Lavabit itself. To review, a Stored Communications Act warrant must have as its object either (1) the contents of a communication (all agree that this warrant is not of that kind) or (2) "a record or other information pertaining to *a subscriber*." 18 U.S.C. §2703(a)-(c) (emphasis added). As was argued in the opening brief (at 19–20), the object of this warrant was something quite different: information that pertained not to a subscriber, but *to Lavabit*.

In response, the government first argues (at 32) that whether Lavabit's encryption keys "pertain to a subscriber" is a "fact-intensive question," which would require the presentation of evidence below.[3] Why exactly that would be so is never explained. There is no factual dispute about what Lavabit's private encryption keys are, who had access to them, how they work, or what they are for. What is disputed is not the *nature* of the information sought (which is a factual question), but whether that information "pertain[s] to a subscriber"—which is a pure question of statutory interpretation. See *Gilbane Bldg. Co. v. Federal Reserve Bank of Richmond*, 80 F.3d 895, 905 (4th Cir. 1996) (court of appeals examines "*de novo* the legal conclusions derived" from factual predicates).

To illustrate this point, imagine that a hearing in district court were held on this issue. The parties would be arguing about what it means for a record or other information to pertain to a subscriber (which is disputed), not the nature of these encryption keys (which is not). No affidavit or testimony can settle that former question. It is a question of law, one this Court is perfectly able to resolve on the current record.

The government also argues (at 32–33) that information may "pertain" to a subscriber even if that information is not known to the subscriber, as Lavabit's private

[3] The government also argues (at 30–31) that our objection to the search warrant's validity is waived. That is incorrect. Lavabit timely objected to the warrant below. App. 66-73. Having made that objection, Lavabit is "not limited to the precise arguments" made below, but can make "any argument in support of that claim." *Yee*, 503 U.S. at 534.

encryption keys are not. That is true, and quite irrelevant. The information sought under the Stored Communications Act (whether known the subscriber or not) must be still be information *about the subscriber*. The government's own examples illustrate exactly this point. For example, the government argues (at 33) that it could seek a warrant for a subscriber's network address (which he might not know). Correct. That is because a subscriber's network address is information about the subscriber, just as his home address or telephone number would be. The government points to a district court decision holding that a record of what cellular-phone towers a subscriber communicated with pertains to that subscriber. *In re Applications*, 509 F. Supp. 2d 76, 79-80 (D. Mass. 2007). Also true, because a list of what towers a subscriber used is still information about that subscriber. And finally, the government says (at 33) that it could obtain a record of telephone calls made by a subscriber, which would also incidentally contain information about other subscribers (because it would show what number the call was placed to). Also true. That is because a record stating "Hal called Mario on November 8" is still a fact *about Hal*, even if it is *also* a fact about Mario.

Lavabit's private encryption keys, however, are totally unlike any of these examples. Those keys do not pertain to any subscriber in any of the senses illustrated by the government's examples. They are the property of the business, and do not tell anyone anything about any subscriber. They do not refer to any subscriber and indeed can be created or replaced quite independently of any subscriber, as the government acknowledges. See Gov't Br. 39. Lavabit's secret encryption keys are important

business records (they are both its property and its cryptographic crown jewels), but they do not pertain to any of its subscribers.

The government never specifies any limiting principle to its view of the statute. What does it mean for information to "pertain to a subscriber" if it is not known to the subscriber, does not refer to a subscriber, does not tell anyone anything about any subscriber, is not specific to any subscriber or group of subscribers, and exists independently from any subscriber? What conceivable class of information could the government *not* seek, if it can seek that? The government suggests no answer to this question; there is none. Its view of the statute would allow it to demand essentially anything from a service provider. And by reading out the statute's "pertaining-to" limitation, the government runs aground "one of the most basic interpretive canons": that a "statute should be construed so that effect is given to all its provisions, so that no part will be inoperative or superfluous, void or insignificant." *Corley v. United States*, 556 U.S. 303, 314 (2009).

Lavabit's interpretation also has the virtue of being consistent with this Court's discussion of the statute in *United States v. Applebaum*, 707 F.3d 283 (4th Cir. 2013). That case explained that the statute provides a way for the government to obtain "a subscriber's name, address, length of subscription, and other like data." *Id.* at 287. The government argues (at 34) this list was not intended to be "exhaustive." That is correct, but misses the point. All of the illustrative items (just like all of the examples in the government's brief, and totally unlike Lavabit's private encryption keys) fit

perfectly within Lavabit's theory of the statute: that it is limited to information *about a subscriber*.

Perhaps realizing this, the government attempts (at 34) something of a purposivist Hail Mary: *Applebaum*, says the government, described the statute as being designed to "protect legitimate law enforcement needs." That is not an argument; it is a rhetorical meat cleaver designed to cut off debate. And even if a free-floating assessment of purpose had greater dignity than the statutory text (which it does not), the government has truncated the quotation; in full, it takes on a rather different character: "As one Senator remarked, the SCA was designed to protect legitimate law enforcement needs *while minimizing intrusions on the privacy of system users as well as the business needs of electronic communications system providers*." 707 F.3d at 287 (citation omitted; emphasis added). Once that deleted context is restored, there is no conflict at all between the statute's purpose and its text: the statute's purpose is to balance the needs of law enforcement and business, and its text does so by restricting what sort of documents the government may get from an innocent third-party business.

B. The warrant imposed an undue burden on Lavabit

In the opening brief, Lavabit argued (at 19–20) that the search warrant impermissibly imposed an undue burden on the company. See 18 U.S.C. §2703(d); *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 171 (1977).[4] The burden was undue

[4] The government concedes (at 37) that "courts may not impose unreasonable burdens in ordering third parties to assist in government investigations" (quoting *New York Telephone*, 707 F.3d at 171), but insists that this is a constitutional requirement

because the company was required to either (1) provide the government its encryption keys in secret, while continuing to take money from customers based on assurances that the system was secure against unmonitored eavesdropping, or (2) provide the keys and shut down. The former choice was inconsistent with Lavabit's ethical obligations to its users, in addition to being a black-letter example of civil fraud; the latter destroyed Mr. Levison's livelihood. In light of Lavabit's proposal to provide the government all of the information to which it was entitled at modest cost, with *no* loss of general customer privacy, forcing Lavabit to this choice was a pointless and unreasonable burden.

In response, the government argues (at 38) that Lavabit's privacy policy stated that the company would comply with lawful court orders—and so, in effect, who cares? But what Lavabit *actually* told its users is that it would disclose information related "to an *individual user*" to the government, if the company were "legally compelled" to do so. App. 91 (emphasis added); see also Privacy Policy, http://lavabit.com/privacy_policy.html (archived version, January 15, 2013; available at http://web.archive.org). The government's request, of course, was not for information about the target of its investigation; it was for secret encryption keys that would have enabled unmonitored eavesdropping of the entire customer base.

(continued…)

rather than a statutory one. The government does not suggest that anything turns on this distinction, and nothing does.

The government also notes (at 38–39) that Lavabit would have been able to obtain new encryption keys—"once court-ordered surveillance [was] complete." The duration of that surveillance, however, was completely uncertain. It was, at minimum, sixty days, and Lavabit can surely be forgiven for thinking that sixty days of fraud and unmonitored eavesdropping is sixty too many. And at any rate, it could have been far more: To keep its surveillance going, all the government would have to do is certify that it was "relevant to an ongoing criminal investigation." 18 U.S.C. §3122(b). That is an incredibly easy standard to meet, as the government well knows; and nothing prevents the government from engaging in *seriatim* certifications every two months for as long as it remained interested in the target of its investigation.

Notwithstanding the government's chiding (at 39), this case has nothing to do with a license to "ignore court orders" or "special protection for business models based on a refusal to cooperate" with law enforcement. That is because Lavabit proposed an alternative course: to record the relevant metadata itself and turn it over promptly to the government, which would have entailed no general loss of customer privacy. Because its software was not already capable of this, Lavabit requested a short period to modify it, and also asked that the government cover implementation costs. Neither of these rather modest requests comes close to earning the government's scare-quotes when it sarcastically refers to Lavabit's "'offer'" (at 41). The government complains (at 40–41) that Lavabit's offer was not made quickly enough, but Lavabit made this offer three days *before* the initial hearing before Judge Hilton—*before*, in

other words, Lavabit's legal objection to the surveillance had been heard by any court. Compare App. 83 with App. 38-53. Moreover, for much of the period noted by the government, Lavabit was without counsel and was not yet fully aware of precisely what the government wanted to do. Once matters became clear, Lavabit's compromise was promptly offered. The government immediately refused it, so it is odd to hear the government complain now (at 41) that the implementation of the offer "still" had not begun weeks after that refusal. Had the government accepted the proposal before the initial hearing in district court, this case might never have come this far.

Finally, the government argues (at 41) that Lavabit did not offer "any basis to evaluate whether [the proposed] compensation" was reasonable. That is because the government requested none. Nor did the government offer any reason to believe Lavabit's estimate was unreasonable; Lavabit proposed to develop custom software to protect its users' privacy while giving the government the information it was authorized to collect, for the princely sum of $2,000. App. 83. It has probably cost the government more to print its briefs in this appeal. At any rate, on the curve of public contracting, Lavabit's offer may qualify as the deal of the century. Cf. Robert Pear, *Health Website Official Tells of White House Briefings*, The New York Times, at A20 (Nov. 13, 2013) (estimating the cost of one government website at $600 million).

C. The warrant did not target the fruits, instrumentalities, or evidence of a crime, as the Fourth Amendment requires

Lavabit argued in the opening brief (at 21–24) that the government's warrant was not founded on probable cause to believe that the "fruits, instrumentalities, or evidence of crime" would be found. See *Zurcher v. Stanford Daily*, 436 U.S. 547, 550 (1978). Instead, the warrant simply seeks totally innocent information from a concededly innocent small business.[5] The Fourth Amendment does not permit that, and so the government's warrant was invalid.

The government does not argue, in response (at 34–36), that Lavabit's private keys were any of those things. Instead, the government argues (at 35) that it may use a search warrant to get any information that would "aid in the apprehension of a suspect." The only authority given for that claim is a quotation from *Warden v. Hayden*, 387 U.S. 294, 307 (1967). But the government takes *Hayden* seriously out of context. What *Hayden* approved was a search for clothing worn by a criminal; the issue before the Court was the validity of the so-called "mere evidence" rule—the "distinction made by some … cases between seizure of items of evidential value only and seizure of instrumentalities, fruits, or contraband." *Id.* at 300. *Hayden* approved of a warrant to "seize evidence" for the purpose of "proving crime." *Id.* at 306. And that is how this Court has always interpreted it; as one decision summarizes *Hayden*, the government

[5] The government argues (at 35)—again—that this argument is waived. The government is—again—incorrect: as described in note 2, *supra*, Lavabit specifically objected to the search warrant on Fourth Amendment grounds. App. 66-73. Having made that timely objection, Lavabit can make "any argument in support of that claim." *Yee*, 503 U.S. at 534.

must show "that there is some nexus between the items to be seized and the criminal activity being investigated." *Doe v. Broderick*, 225 F.3d 440, 451 (4th Cir. 2000). That required nexus is absent here, and the immediately prior sentence in *Doe* states exactly the proposition upon which we rely: "Probable cause exists when there are reasonably trustworthy facts which, given the totality of the circumstances, are sufficient to lead a prudent person to believe that the items sought constitute *fruits, instrumentalities, or evidence of crime* and will be present at the time and place of the search." *Ibid.* (quoting *United States v. Suarez*, 906 F.2d 977, 984 (4th Cir. 1990)) (emphasis added).

The government's expansive reading of *Hayden* has already been rejected once by a district court in this circuit. See *In re Application of U.S. for an Order Authorizing Disclosure of Location Information*, 849 F. Supp. 2d 526, 560 (D. Md. 2011) (noting the government's "almost exclusive[]" reliance on *Hayden*, and rejecting the government's reading of it). In that case, "the government admitted at the hearing it was unable to provide any explicit substantive support for its reading of *Hayden* in factually apposite cases, treatises or law reviews"—its brief here does not improve in that regard, as will be discussed below. *Id.* at 561. And the district court observed that "the response to *Hayden* of the Advisory Committee on Criminal Rules is instructive," in that the Committee "did not seek to amend Rule 41 to clarify that a search warrant may be used to obtain evidence that will aid in the apprehension of a defendant," but rather only to provide that "search warrants may issue for evidence of the commission of a crime." *Id.* at 561 n.19. As the district court summarized the law then: "The Court

could find no case where a search warrant was issued to obtain information to aid in the apprehension of a criminal where the sought-for information would not be evidence of a crime." *Id.* at 562.

So while *Hayden* does speak of evidence that would aid in the "apprehension" of criminals, "[l]egal pronouncements do not live isolated from the facts; they can only be understood in the context of the facts presented."*Ibid. Hayden* never considered, and no case since has approved, a search of a totally innocent third party for information like Lavabit's private keys—information that is (1) legal to possess, (2) does not prove that any crime occurred, (3) was not the fruit of any crime, and (4) was not used to commit any crime. *Hayden* should be understood, as it always has been, to reject the "mere evidence" rule. No more.

And as the district court in *In re Application* noted, the government has no support for its expansive interpretation of *Hayden*'s dictum. The cases it cites simply illustrate that Lavabit's description of the law is correct. The government cites (at 35):

- A case permitting the seizure of apartment keys because they "constituted evidence of appellant's constructive possession of the narcotics found," and were "instrumentalities" of the underlying drug crime. *United States v. Thompson*, 495 F.2d 165, 169 (D.C. Cir. 1974). But of course, Lavabit's encryption keys are not alleged to be "evidence" that the government's target has done anything, nor are they alleged to be "instrumentalities" of the target's crimes.
- A district court case from another circuit that approved a warrant for a suspect's cell-phone records, which were used to track his location. *In re Smartphone Geolocation Data Application*, No. 13-MJ-242, 2013 WL 5583711 (E.D.N.Y. May 1,

2013). For the reasons described above, this decision is likely incorrect, and explicitly broke with the Maryland district court's opinion in *In re Application*. But even this case only approved searching for a *suspect's* cell-phone records to aid in his apprehension; it did not bless the far more radical course the government proposes here. The government's request in this case is more like tracking the cell phone of an innocent third party known to work in the same office as a criminal suspect.

- Three district-court cases, none from this circuit, that approved the seizure of encryption keys. See Gov't Br. 36. None of these cases discuss or decide the Fourth Amendment objection raised here. That is because all of them deal with encryption keys that belonged *to the defendant*, which were being used to conceal what he had done—they were, in other words, instrumentalities the defendant was using to commit his crimes. See *United States v. Scarfo*, 180 F. Supp. 2d 572, 577 (D.N.J. 2001) (defendant encrypted illegal business records with his encryption keys); *United States v. Sutton*, No. 5:08-CR-40, 2009 WL 481411 (M.D. Ga. Feb. 25, 2009) (approving search of defendant's computer for evidence of his fraud); *United States v. Simpson*, No. 3:09-CR-249, 2011 WL 721912 (N.D. Tex. Mar. 2, 2011) (approving search of defendant's home and computers). (It is not even clear that anything was encrypted in *Sutton* or *Simpson*; the district court decisions mention "encryption" only in the description of the warrant's boilerplate language.)

This is thin gruel. And it is the best the government has.

The government cannot find more authority for its claimed power because it does not exist. The usual mechanism for seeking useful information from innocent third parties is a subpoena. And the difference is crucial; when an innocent third party is commanded to produce its business records with a subpoena, it enjoys some protection in the form of a motion to quash. But if the government's theory of the

Fourth Amendment were correct, police could get search warrants for all manner of bizarre things. (Could the government send FBI agents to its target's mother, armed with a search warrant for her family photos—which of course would be very useful in generating a description of their target?) This Court should not be the first to sanction this large and unnecessary expansion of government power.

D. The warrant permitted general rummaging through other subscribers' communications

Finally, Lavabit argued in the opening brief (at 24–27) that the warrant was also invalid because it permitted—and the government's investigation explicitly contemplated—examining *all* the communications data coming in and out of Lavabit's servers. But examining the communications of hundreds of thousands of innocent people absent any suspicion is an unreasonable search. In response, the government concedes (at 43) that the communications data will all be examined—but, we are told, only "momentarily," and only by its surveillance device; the government promises that the communications of innocent people will not "reach[] any human eye."

For this argument to be successful, the government would need two things, neither of which it has. First, it would need some evidence for the factual premise—some reason to believe, in other words, that its description of its device is accurate. Perhaps it is, but the government points to no evidence of it. That is troubling, because as has now become well known, the government (1) maintains a variety of

private, exotic theories about when it is lawful for it to capture and retain electronic communications, and (2) does not always observe even court-ordered limits on its surveillance, as Judge Bates has observed in his capacity of as a FISA court judge. See *(Redacted)*, *No. PR/TT (Redacted)*, at 14 (FISA Ct., Date Redacted), available at http://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf (discussing the government's admission that it "had regularly accessed" metadata "that had not been approved"). So it is not too much to ask that the government substantiate its claim with more than a bald statement in a legal brief.

Second, and perhaps more important, the government would need some legal authority for the proposition that it is entitled to intercept the communications of an innocent person, so long as the interception is brief and done only by a computer without subsequent human examination. No such authority exists. The ordinary legal framework of the Fourth Amendment points in exactly the opposite direction. (1) Searches are presumptively unreasonable if done without suspicion of wrongdoing, see *Chandler v. Miller*, 520 U.S. 305, 308 (1997); (2) intercepting a communication is a search, see *Berger v. New York*, 388 U.S. 41, 51 (1967); (3) therefore, intercepting all of Lavabit's traffic is unreasonable, because it is done without any suspicion of wrongdoing by the vast majority of the people affected. The government argues in a footnote (at 44 n.11) that its device does not conduct "searches" to the extent it only examines the "envelope information" about the email—its sender, recipient, subject

line, etc.—but even if that were correct, the device necessarily intercepts a great deal more than that.

Therefore, the government misapprehends the argument (at 45–47) when it objects at length to Lavabit's "conjecture that the government will execute a search warrant illegally," and insists that such conjecture "is not grounds to invalidate a warrant." The point is that what the warrant *authorizes* is illegal: the suspicionless interception of hundreds of thousands of innocent people's email by a government surveillance device, absent any suspicion of wrongdoing on their part. When this Court was confronted with a warrant that authorized the seizure of legitimate documents from a company that was (unlike here) "permeated with fraud," it did not hesitate to find the warrant invalid. *United States v. Oloyede*, 982 F.2d 133, 141 (4th Cir. 1992) (per curiam). A fortiori, scanning all the communications of a legitimate business is even worse.

CONCLUSION

It bears repeating: the government has no general entitlement to search through the information of an innocent business. It may do so only to the extent that the law and Constitution permit. The government proposed, in this case, to search through a vast amount of data to find a tiny amount relevant to its investigation, with no oversight from anyone, at a time when the government's theories of its own surveillance power are at their apex. It ruined a small business in doing so, despite the existence of a far more reasonable alternative, which would have given the

government access to only that information that it was authorized to collect. The surveillance statutes and the Fourth Amendment do not allow the government to chart this course. The judgment of the district court should therefore be reversed.

Dated: November 22, 2013 Respectfully submitted,

Jesse R. Binnall
BRONLEY & BINNALL, PLLC
10387 Main Street
Suite 201
Fairfax, VA 22030
703.229.0335

/s/ Ian Samuel
Ian Samuel
JONES DAY
222 E. 41st Street
New York, NY
212.326.3808

Marcia Hoffman
LAW OFFICE OF MARCIA HOFFMAN
25 Taylor Street
San Francisco, CA 94102
415.830.6664

David Warrington
Laurin Mills
LECLAIRRYAN
2318 Mill Road
Suite 1100
Alexandria, VA 22314
703.647.5926

Counsel for Party-in-Interest-Appellant

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because:

this brief contains 6,873 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because:

this brief has been prepared in a proportional spaced typeface using Microsoft Word in 14 point Garamond.

Dated: November 22, 2013

/s/ Ian Samuel
Ian Samuel

CERTIFICATE OF SERVICE

On November 22, 2013, the foregoing document was filed on the CM/ECF system, which served the document on all parties or their counsel.

Dated: November 22, 2013

/s/ Ian Samuel
Ian Samuel