NO. 18-50440

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

PLAINTIFF–APPELLEE,

v.

LUKE WILSON

DEFENDANT–APPELLANT

On Appeal from the United States District Court
for the Southern District of California
No. 15-cr-02838-GPC
The Honorable Gonzalo P. Curiel, United States District Court Judge

# BRIEF OF AMICI CURIAE ELECTRONIC FRONTIER FOUNDATION AND AMERICAN CIVIL LIBERTIES UNION FOUNDATION IN SUPPORT OF DEFENDANT–APPELLANT

Jennifer Stisa Granick
*Counsel of Record*
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111
(415) 343-0758
jgranick@aclu.org

Brett Max Kaufman
Nathan Freed Wessler
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street
New York, NY 10004
(212) 549-2500

Jennifer Lynch
*Counsel of Record*
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
jlynch@eff.org

*Attorneys for Amici Curiae Electronic Frontier Foundation and American Civil Liberties Union*

## CORPORATE DISCLOSURE STATEMENT

Pursuant to Rules 26.1 and 29(a)(4)(A) of the Federal Rules of Appellate Procedure, amici curiae state that they do not have a parent corporation and that no publicly held corporation owns 10% or more of their stock.

Pursuant to Federal Rule of Appellate Procedure Rule 29(a)(4)(E), amici curiae certify that no person or entity, other than amici, their members, or their counsel, made a monetary contribution to the preparation or submission of this brief or authored this brief in whole or in part.

# TABLE OF CONTENTS

# TABLE OF AUTHORITIES

## Cases

**Constitutional Provisions**



**Legislative Materials**



**Other Authorities**

## STATEMENT OF INTEREST[1]

Amicus curiae the Electronic Frontier Foundation ("EFF") is a member-supported, non-profit civil liberties organization that has worked to protect free speech and privacy rights in the online and digital world for nearly thirty years. With roughly 40,000 active donors, EFF represents technology users' interests in court cases and broader policy debates, and actively encourages and challenges the government and courts to support privacy and safeguard individual autonomy as emerging technologies become more prevalent in society. EFF regularly participates as amicus in the Supreme Court, this Court, and other courts in cases addressing the Fourth Amendment and its application to new technologies. *See, e.g.*, *Carpenter v. United States,* 138 S. Ct. 2206 (2018); *Riley v. California*, 573 U.S. 373 (2014); *City of Ontario v. Quon*, 560 U.S. 746 (2010); *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization with more than two million members and supporters dedicated to the principles of liberty and equality embodied in the Constitution and our nation's civil rights laws. Since its founding in 1920, the ACLU has frequently

[1] Pursuant to Federal Rule of Appellate Procedure Rule 29(a), no counsel for a party authored this brief in whole or in part, and no person other than amicus or their counsel has made any monetary contributions to fund the preparation or submission of this brief. Pursuant to Federal Rule of Appellate Procedure Rule 29(a)(2), amici represent that all parties have consented to the filing of this brief.

appeared before the Supreme Court and other federal courts in numerous cases implicating Americans' right to privacy, including as counsel in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and as amicus in *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

## INTRODUCTION

As the district court recognized in this case, the Fourth Amendment protects the contents of email. Excerpts of Record ("ER") at 198. (citing *United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2008)). This is because email "is the technological scion of tangible mail, and it plays an indispensable part in the Information Age." *United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010). Since *Warshak*, courts have routinely held that individuals have a reasonable expectation of privacy in their email held in accounts operated by third party providers. The Supreme Court has agreed, at least in dicta; in the Court's recent opinion in *United States v. Carpenter*, every Justice authored or joined an opinion acknowledging that the Fourth Amendment protects the content of stored digital files. *See* 138 S. Ct. 2206, 2222 (2018) (majority op., Roberts, C. J., joined by Ginsberg, Breyer, Sotomayor, and Kagan, JJ.); *id.* at 2230 (Kennedy, J., dissenting, joined by Thomas and Alito, JJ.); *id.* at 2262, 2269 (Gorsuch, J., dissenting).

Yet, the district court opined that when people "agree" to an email service provider's terms of service ("TOS") stating that the provider may monitor or analyze user accounts for illegal or unwanted behavior, they lose their reasonable expectation of privacy in any content stored in that account. ER at 198-200. This analysis would instead apply to any and all emails, files, and attachments maintained with the service provider, in this case Google, one of the largest email

service providers in the United States. Not only would it vitiate Fourth Amendment protections for hundreds of thousands, or even millions of people, it would mean that a private company's TOS trumps Fourth Amendment protections for *all* content maintained with the provider. This is inconsistent with public expectations, well-recognized Fourth Amendment case law, and Supreme Court dicta. If adopted by this Court, it would undermine fundamental privacy protections in communication media used by nearly all Americans.

The lower court opined that the specific language in Google's TOS allowing it to monitor users' content and remove it if it was "illegal" or otherwise violated the TOS defeated Wilson's reasonable expectation of privacy in that content. However, while a TOS may govern the relationship between the provider and the user, such form contracts cannot extinguish a user's constitutional rights as against the government. *United States v. Byrd*, 138 S. Ct. 1518, 1529 (2018). Similarly, a provider's mere ability to access its users' content does not extinguish those rights either. *Warshak*, 631 F.3d at 286–87; *In re Grand Jury Subpoena, JK-15-029*, 828 F.3d 1083, 1090 (9th Cir. 2016).

The government suggested an alternative approach, one that it may raise again on appeal. In the court below, it argued that Wilson had no expectation of privacy in his account information once Google terminated his account for uploading contraband material. The district judge did not address this argument,

and this Court should not adopt it either. As with rental cars, individuals retain an expectation of privacy in their private papers and property, even if a provider unilaterally decides to terminate their account. *See, e.g.*, *United States v. Henderson*, 241 F.3d 638, 647 (9th Cir. 2000) (lessee maintains a reasonable expectation of privacy in a rental car even after the rental agreement has expired).

Under both the District Court's and the government's rationales, Fourth Amendment protections would rise and fall depending on take-it-or-leave-it notices drafted by dominant communications platforms and the unilateral actions the companies take pursuant to those notices. Although this case involves child pornography, neither approach could be cabined to child pornography cases. The district judge reserved the question of whether Mr. Wilson had a legitimate expectation of privacy in data other than the four contraband files he uploaded, since the officer did not review any other information. But from a Fourth Amendment standpoint, there is no difference between the privacy interests in the four files that Google forwarded and which an officer decided to review, and the tens of thousands he did not review.[2] Similarly, providers reserve the right to terminate accounts for many reasons unrelated to child pornography, including if

[2] If the four files are to be treated differently for Fourth Amendment purposes, it would be because of operation of the private search doctrine, *see* ER 203-206, not because the defendant lacks a reasonable expectation of privacy in them. Amici take no position on how the private search doctrine applies to the facts of this case.

content is merely "objectionable" or violates copyrights. Under the government's view, a service provider would have the ultimate power to determine individuals' constitutional privacy and property interests in their personal documents. If the provider terminates the account, even for legal but undesirable activity, Fourth Amendment protection would dissolve. This would lead to absurd results and would be contrary to *Warshak* and to Supreme Court dicta in *Carpenter*. Surely when the Justices in *Carpenter* were writing approvingly of individual privacy rights in email, they were not excluding people who use Gmail, one of the most popular email services in the United States and around the world.[3]

The district court ultimately decided this case under an alternate theory, and its statements that Gmail users have no Fourth Amendment right in their email messages are dicta. However, should this Court adopt this reasoning—and the government may argue that this dicta provides an alternative basis for affirmance here—it would have broad impact. Under the lower court's rationale, the vast majority of email users would have no reasonable expectation of privacy in their entire account—likely comprising thousands of emails describing sensitive and intimate details of that user's life. This would mean that law enforcement would be able to warrantlessly collect almost all email and other personal files stored online;

[3] Litmus, Email Client Market Share (February 2019), https://emailclientmarketshare.com/.

it would eviscerate privacy interests in email and other private files.

This Court should reject both rationales. Instead, this Court should make clear that people have a reasonable expectation of privacy in their email and uploaded files, even if contraband, despite monitoring warnings in terms of service or privacy policies, and regardless of whether the user's account is terminated or not.

## ARGUMENT

### I. Courts Widely Recognize Fourth Amendment Protections for Email and Other Stored Documents.

By now, most courts to address the question recognize that users have a Fourth Amendment-protected interest in the contents of their digital communications. Email and other electronic communications have in recent years far surpassed, or even entirely replaced, letters and phone calls as a means of communication for most people and have become "so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification." *City of Ontario v. Quon*, 560 U.S. 746, 760 (2010). Because people now conduct much, if not all, of their personal and professional correspondence electronically, obtaining access to a person's email account allows the government to examine not just a handful of selected letters in one's letterbox, but years worth of communications. One 2013 study found that, on average, people have around 8,000 emails stored with their service provider, and

about 20 percent of users have more than 21,000 emails stored in their inbox.[4]

Email is just a subset of the sensitive and extensive collections of electronic documents and files people store online today. Like the modern cellphone, online accounts today can contain "a digital record of nearly every aspect of [people's] lives—from the mundane to the intimate." *Riley v. California*, 573 U.S. 373, 395 (2014). Like the digital devices at issue in *United States v. Cotterman*, digital communications "contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails." 709 F.3d 952, 964 (9th Cir. 2013) (en banc). "Personal email can, and often does, contain all the information once found in the 'papers and effects' mentioned explicitly in the Fourth Amendment." *In re Grand Jury Subpoena*, 828 F.3d at 1090.

For these reasons, every Justice of the Supreme Court has suggested that the Fourth Amendment protects the content of digital documents stored with third parties. *See Carpenter*, 138 S. Ct. 2206, 2222 (2018) (majority op.) ("If the third-party doctrine does not apply to the 'modern-day equivalents of an individual's own 'papers' or 'effects,'' then the clear implication is that the documents should receive full Fourth Amendment protection."); *id*. at 2230 (Kennedy, J., dissenting) (Case law permitting warrantless access to records "may not apply when the

[4] Dave Troy, *The Truth About Email*, Pando.com (Apr. 5, 2013), https://pando.com/2013/04/05/the-truth-about-email-whats-a-normal-inbox.

Government obtains the modern-day equivalents of an individual's own 'papers' or 'effects,' even when those papers or effects are held by a third party."); *id*. at 2262, 2269 (Gorsuch, J., dissenting) ("Even our most private documents—those that, in other eras, we would have locked safely in a desk drawer or destroyed—now reside on third party servers. *Smith* and *Miller* teach that the police can review all of this material, on the theory that no one reasonably expects any of it will be kept private. But no one believes that, if they ever did." (citing *Smith v. Maryland*, 442 U.S. 735 (1979) and *United States v. Miller*, 425 U.S. 435 (1976))).

Since *Warshak*, all of the major electronic communications service providers, including Google, require a warrant before turning over the contents of their users' accounts to the government.[5] And it has been Department of Justice policy since at least 2013 to seek warrants to access the contents of online messages.[6]

---

[5] *See* Rainey Reitman, *Who Has Your Back? Government Data Requests 2017*, EFF (July 10, 2017), https://www.eff.org/who-has-your-back-2017#best-practices (survey of twenty-six technology companies and their policies on government access to user data); *see also, e.g.*, Google, *Legal process for user data requests FAQs*, https://support.google.com/transparencyreport/answer/7381738?hl=en (warrant required for contents of Gmail); Microsoft, *Law Enforcement Requests Report*, https://www.microsoft.com/en-us/about/corporate-responsibility/lerr (warrant required for content of customer accounts); Facebook, *Information for Law Enforcement Authorities*, https://www.facebook.com/safety/groups/law/guidelines/ (warrant required for "stored contents of any account, which may include messages, photos, videos, timeline posts and location information").

[6] *See* H.R. Rep. No. 114-528, at 9 (April 26, 2016) (noting, "[s]oon after the

## II. The Ability of a Third Party Service Provider to Access Stored Files Does Not Defeat the User's Reasonable Expectation of Privacy.

Individuals enjoy an expectation of privacy in digital files even though third parties facilitate the sending and receiving of messages and store the content. That is because merely entrusting digital "papers" and "effects" to an intermediary does not defeat the reasonable expectation that the contents of the materials will remain private. *Smith*, 442 U.S. at 741 (distinguishing constitutional protection for contents of conversation from numbers dialed). This has always been true for physical mail, even though at any point a mail carrier could open a letter and examine its contents. *Warshak*, 631 F.3d at 285 (*citing United States v. Jacobsen*, 466 U.S. 109, 114 (1984)). Likewise, since the Supreme Court's ruling in *Katz v United States,* 389 U.S. 347 (1967*),* it has been "abundantly clear that telephone conversations . . . are fully protected by the Fourth and Fourteenth Amendments"—even though the telephone company could "listen in when reasonably necessary to 'protect themselves and their properties against the improper and illegal use of their facilities.'" *Warshak,* 631 F.3d at 285, 287 (citing *Smith*, 442 U.S. at 746; *Bubis v. United States*, 384 F.2d 643 (9th Cir. 1967)). As *Warshak* recognized, third-party Internet service providers ("ISPs") are the "functional equivalent" of post offices or phone companies; they make "email

---

[*Warshak*] decision, the Department of Justice began using warrants for email in all criminal cases. That practice became Department policy in 2013.").

communication possible. Emails must pass through an ISP's servers to reach their intended recipient." 631 F.3d at 286. Therefore, as with letters and phone calls, the ability of a third-party service provider to access individuals' emails does not diminish the reasonableness of users' trust in the privacy of their emails. *Id.* at 286–87; *accord In re Grand Jury Subpoena*, 828 F.3d at 1090 (explaining that "email should be treated like physical mail for purposes of determining whether an individual has a reasonable expectation of privacy in its content," and that a third party's "current possession of the emails does not vitiate that claim"). Most recently, in *Carpenter*, the Supreme Court made clear that one's reasonable expectation of privacy in information as against the police (or, for that matter, the public) is not automatically defeated merely because a third party has access to or control over that information. 138 S. Ct. at 2219–20.

As the *Warshak* court noted, Fourth Amendment protection for private documents stored with third parties finds further support "in the application of Fourth Amendment doctrine to rented space." 631 F.3d at 287. *Warshak* recognized:

> Hotel guests, for example, have a reasonable expectation of privacy in their rooms. This is so even though maids routinely enter hotel rooms to replace the towels and tidy the furniture. Similarly, tenants have a legitimate expectation of privacy in their apartments. That expectation persists, regardless of the incursions of handymen to fix leaky faucets.

*Id.* at 287 (citations omitted). *See Stoner v. California*, 376 U.S. 483, 490 (1964);

*Chapman v. United States*, 365 U.S. 610 (1961); *see also Carpenter*, 138 S. Ct. at 2268 (Gorsuch, J., dissenting) (discussing the law of bailments and noting "the fact that a third party has access to or possession of your papers and effects does not necessarily eliminate your interest in them").

The district court's dicta in this case runs counter to *Warshak*'s reasoning, and disregards the fact that almost every individual treats her email account as private, even though the company that provides her email service has access to it for limited purposes. From another vantage, the reasoning stands for the counterproductive proposition that a private email provider must choose between protecting its users' privacy interests and protecting its own business. If a provider chooses to police its platform for illegality or other misconduct, it vitiates its users' expectations of privacy and leaves them open to warrantless and suspicionless searches by the government. But if it chooses the alternative, the company could end up allowing criminal conduct to run on its service unabated.

Mr. Wilson had a reasonable expectation of privacy in the contents of his emails and files stored with Google, despite the company's ability to access them.

## III. A Service Provider's TOS Does Not Defeat Its Users' Reasonable Expectations of Privacy in their Email or Digital Papers.

The court below held that the government's warrantless search of four attachments Mr. Wilson uploaded to his Gmail account did not violate the Fourth Amendment because the investigator did not exceed the scope of Google's private

search. This holding assumes, correctly, that Mr. Wilson had an expectation of privacy in his email generally and in those four attachments specifically. Nevertheless, the district court also opined in dicta that Mr. Wilson—and by extension any Google email user—cannot have a reasonable expectation of privacy in contraband files uploaded to an email account because Google's TOS advised him that it could monitor user accounts for violations of its policies and illegal conduct. ER 199. However, while a private contract like Google's TOS may govern the provider's relationship with the user, it cannot vitiate the user's Fourth Amendment rights.[7]

### A. Monitoring Policies Do Not Extinguish a User's Reasonable Expectation of Privacy.

People have an expectation of privacy in their digital letters, papers, and effects even when their service provider has the ability to monitor these records. *Supra* II. The expectation of privacy analysis is intended to describe "well-recognized Fourth Amendment freedoms," *Smith*, 442 U.S. at 740 n.5, not the interests of private businesses as advanced by terms that are often buried on a website or in an app. Users' Fourth Amendment-protected expectations of privacy are not upended when third-party providers give notice that they may exercise their

[7] The district court did not consider the entirety of Google's TOS. The TOS announces that the company may monitor user content. However, it goes on to say: "that does not mean necessarily mean that we review content, so please don't assume that we do." ER 82.

capability to access or monitor the user's account. The fact that a private entity reserves the right to interdict illegal activity to protect its own business interests does not enable *the government* to search emails and documents on the platform without a warrant. For example, in *Warshak*, the email service provider reserved the right to monitor subscriber information under its Acceptable Use Policy. 631 F.3d at 287. Nevertheless, the Sixth Circuit found a reasonable expectation of privacy. For business reasons, communications companies almost always notify users that they may conduct private searches as part of their goal to identify and stop illegal activity, or even to merely to protect their business from objectionable conduct or content. These reservations of rights are almost never negotiated, and users have no choice but to click "I agree" just to engage in activities fundamental to modern life. *Riley*, 573 U. S. at 385.[8]

Just last term, the Supreme Court rejected the assumptions that underlie the district court's dicta. In *United States v. Byrd*, 138 S. Ct. 1518 (2018), the police stopped and searched a rental car driven by someone who was not on the rental

[8] Providers' TOS almost universally allow them to monitor for certain purposes, so a rule following the district court's dicta and the government's argument would mean that only the rare individual who knows how to set up and run their own private email server would maintain a reasonable expectation of privacy in their emails. That position would come as a surprise to the hundreds of millions of Americans who rely on commercial email services. *See* Taylor Kerns, *Gmail Now Has More than 1.5 Billion Active Users*, Android Police (Oct. 26, 2018), https://www.androidpolice.com/2018/10/26/gmail-now-1-5-billion-active-users/.

agreement but was given permission to drive by the renter, and discovered heroin. The Court held that drivers have a reasonable expectation of privacy in a rental car even when they are driving the car in violation of the rental agreement. Car-rental agreements, wrote the Court, are filled with long lists of restrictions that have nothing to do with a driver's reasonable expectation of privacy in the rental car. Even a serious violation of the rental agreement has no impact on expectation of privacy. Rental agreements, like terms of service, "concern risk allocation between private parties. . . . But that risk allocation has little to do with whether one would have a reasonable expectation of privacy in the rental car if, for example, he or she otherwise has lawful possession of and control over the car." *Id.* at 1529. Since the defendant in *Byrd* was lawfully in possession of the car, despite the fact that he was violating a private agreement, he had an expectation of privacy. The Fourth Amendment therefore applied to the government's search.

Just as the Supreme Court has cautioned "that arcane distinctions developed in property and tort law . . . ought not to control" the analysis of who has a "legally sufficient interest in a place" for Fourth Amendment purposes, *Rakas v. Illinois*, 439 U.S. 128, 142–43 (1978), courts have repeatedly declined to find private contracts dispositive of individuals' expectations of privacy. In *Smith*, for example, the Supreme Court noted, "[w]e are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here) the pattern of protection

would be dictated by billing practices of a private corporation." *Smith*, 442 U.S. at 745. Similarly, in *United States v. Thomas*, this Circuit held that the "technical violation of a leasing contract" is insufficient to vitiate an unauthorized renter's legitimate expectation of privacy in a rental car. 447 F.3d 1191, 1198 (9th Cir. 2006). And in *United States v. Owens*, the Tenth Circuit did not let a motel's private terms govern the lodger's expectation of privacy, noting, "[a]ll motel guests cannot be expected to be familiar with the detailed internal policies and bookkeeping procedures of the inns where they lodge." 782 F.2d 146, 150 (10th Cir. 1986).

If the district court were right in this case, Fourth Amendment protections would rise and fall depending on different courts' interpretations of different service providers' usage policies at different points in time. Customers of one company would enjoy Fourth Amendment rights, while customers of another, including Google, would not. Supreme Court precedent could be reversed by a commercial privacy policy. That is not workable for the government or the public and cannot be right. *See Smith*, 442 U.S. at 745.

### B. The District Court's Reasoning Could Leave All Email Messages, Not Just Contraband Files, Unprotected by the Fourth Amendment.

The district court suggests there may be a distinction between Mr. Wilson's expectation of privacy in the four uploaded contraband images and in the rest of

his email account. ER 200 n.7. But that is a distinction without a difference. Google advises its users that it may monitor or analyze their *entire* account. ER 82, 83. If that advisement defeats the user's expectation of privacy, it would do so for the entire account. Nor does it matter that, when conducting this account monitoring, some files in that account are contraband. The Supreme Court has held that "a warrantless search [can]not be characterized as reasonable simply because, after the official invasion of privacy occurred, contraband is discovered." *Jacobsen*, 466 U.S. at 114. Individuals retain a reasonable expectation of privacy in their papers, effects, and houses even when criminal activity is ongoing. *See e.g. Byrd*, 138 S. Ct. 1518 (reasonable expectation of privacy in rental car containing heroin); *Jacobsen*, 466 U.S. at 114 (reasonable expectation of privacy in parcel containing cocaine); *Owens*, (reasonable expectation of privacy in hotel room containing cocaine). The same is true with Mr. Wilson's Google account. There is no logical line to draw that leaves evidence of his illegal activity outside of the Fourth Amendment, and the rest of the private, sensitive, intimate details of one's life held in an online account within its protections.

## IV. A Reasonable Expectation of Privacy Does Not Expire Just Because an Account Is Terminated or an Account Holder's Access Is Cut Off.

In its brief below, the government also pointed to the fact that Google had terminated Wilson's account upon discovering the illegal files and argued this vitiated Mr. Wilson's Fourth Amendment rights. The terms of service announced

by American email providers are often quite broad and uniformly give the provider the power to terminate accounts unilaterally, for reasons far less serious than sending images of child pornography. For instance, Google reserves the right to terminate a user's Gmail account not only for known violations of its policies—which include broad prohibitions against conducting or promoting any illegal activity and intimidating others[9]—but even while it investigates suspected misconduct.[10] Yahoo's TOS reserves the right to terminate users' accounts "for any reason, including, but not limited to, violation of these Terms, court order, or inactivity." TOS violations include such activities as sending content that is "racially, ethnically, or otherwise objectionable[;]" violates the "copyright or other proprietary rights of any person or entity[;]" or constitutes unsolicited advertising.[11] Microsoft's TOS allows it to terminate access to certain "Communications Services [including email] at any time, without notice, for any reason whatsoever."[12] Microsoft also reserves the right to change its terms of use

[9] Google, *Gmail Program Policies*, https://www.google.com/gmail/about/policy/.

[10] Google, *Google Terms of Service*, https://www.google.com/intl/en/policies/terms/.

[11] Oath, *Oath Terms of Service*, https://policies.oath.com/us/en/oath/terms/otos/index.html.

[12] Microsoft, *docs.microsoft.com - Terms of use*, https://docs.microsoft.com/en-us/legal/termsofuse.

without any notice to the user.[13]

In other words, actions that could cause a provider to terminate an account for TOS violations include not just criminal activity such as distributing child pornography but also—as defined solely by the provider—sending an email containing a racial epithet, sharing a news article with work colleagues without permission from the copyright holder, or marketing a small business to a large group of friends without their advance consent. While some might find activities such as these highly objectionable or annoying, that should not be enough to vitiate a Fourth Amendment right. Not only would that mean that the Fourth Amendment's warrant requirement turned on contract terms, its application would turn on the unilateral actions of service providers.

Courts have recognized that an individual's expectation of privacy survives the termination of a contractual relationship in other analogous contexts. Both this Circuit and the Eleventh Circuit have found, for example, that a lessee maintains a reasonable expectation of privacy in a rental car even after the rental agreement has expired. *See Henderson*, 241 F.3d at 647; *United States v. Cooper*, 133 F.3d 1394, 1402 (11th Cir. 1998); *see also Owens*, 782 F.2d at 150.

Nor could Wilson's loss of access to and control of his Google account on its own eliminate his expectation of privacy in his email as against the government.

[13] *Id.*

Likening email to a closed container, this Court has held that the fact that a third party controls access to one's email is insufficient to vitiate a legitimate expectation of privacy in the email. *In re Grand Jury Subpoena*, 828 F.3d at 1091. This makes sense—if a sealed letter sent through the mail falls into the wrong hands (thus terminating the ability of the letter writer to access it), that does not, absent something more, nullify the letter writer's expectation of privacy in the letter's contents vis-à-vis the government.

Of course, if a non-governmental entity in possession of a letter or email decided to open it and report its contents to the government, the "private search" doctrine may apply. *Jacobsen,* 466 U.S. 109; *Walter v. United States*, 447 U.S. 649 (1980). The private search doctrine holds that the Fourth Amendment "is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official." *Jacobsen*, 466 U.S. at 113–14 (internal quotation omitted). The government may make use of the fruits of a private search, but it "may not exceed the scope of the private search unless it has the right to make an independent search." *Id.* at 116 (quoting *Walter*, 447 U.S. at 657 (Stevens, J.)).

The line drawn in private search cases such as *Walter* and *Jacobsen* would be irrelevant if mere loss of control of a package or letter were enough to defeat an

expectation of privacy. In *Walter*, for example, if the defendant's expectation of privacy in the film reels he sent through private mail were overcome once they were delivered to an unintended recipient (and thus once they were out of his control), the Court would not have needed to go the next step to determine whether law enforcement's viewing of those films expanded the search beyond the recipient's opening of the sealed boxes. Similarly, in *United States v. Lichtenberger*, 786 F.3d 478 (6th Cir. 2015), the Sixth Circuit would not have needed to determine whether the government's search of Lichtenberger's computer exceeded the scope of a private party's earlier search if Lichtenberger lost a reasonable expectation of privacy in his computer's contents when a private party seized control of it and changed the password so he could not access it. *Id.* at 483–84. As the reasoning in these cases demonstrates, Google's termination of the defendant's account cannot defeat his expectation of privacy.

## V. Adopting the District Court's Reasoning Would Reinstate the Third-Party Doctrine for Email, Create a Split of Authority with the Sixth Circuit, and Ignore Supreme Court Rulings.

Courts, the public, and major Internet companies unanimously recognize that people expect their email communications to remain private, and the government regularly obtains a warrant before trying to access a person's email. Should this court find that a service provider could, through its TOS, unilaterally abrogate this expectation of privacy, it would be a radical departure from the privacy that people

have long expected and which the Supreme Court has acknowledged with respect to their personal communications. It would also create a split of authority with the Sixth Circuit.

The court below cited one of this Court's cases, *United States v. Heckenkamp*, 482 F.3d 1142 (9th Cir. 2007), to suggest that there may be some terms of service that could obviate a reasonable expectation of privacy. In *Heckenkamp*, the defendant connected his personal computer to his college's network, which had a policy advising that there were limited instances in which university administrators may access network-attached computers in order to protect the university's systems. This policy did not defeat Heckenkamp's Fourth Amendment interests in his computer, though this Court suggested that a policy advising the user "that information transmitted through the network is not confidential and that the systems administrators may monitor communications transmitted by the user" might. *Id.* at 1147.

But three years after *Heckenkamp*, the Supreme Court cautioned against broad holdings that would define employees' privacy expectations vis–à-vis employer-provided technological equipment, even when the applicable policy is even more concrete than this Court's hypothetical policy in *Heckencamp*. *See Quon*, 560 U.S. 746. In *Quon*, the Court refrained from assessing the plaintiff's expectation of privacy in his pager messages despite his employer's, the Ontario,

California Police Department, clear policy to the contrary: "[u]sers should have no expectation of privacy or confidentiality when using" city resources. *Id*. at 758.

This Court should similarly refrain. It is understandable that courts would want to leave open the possibility that under some future and unknown set of facts, they may reach a different conclusion, but this is not that case. The relationship between Internet users and commercial service providers like Google are quite different from the relationship between students like Heckenkamp and their universities, and between employees like Quon and his government employer.

In *Warshak*, the Sixth Circuit rejected the application of the third-party doctrine to email because, as with phone calls and physical letters, it is reasonable to expect privacy in the contents of communications, despite contract terms allowing for third-party access. 631 F.3d at 287. Although the Sixth Circuit said it was "unwilling to hold that a subscriber agreement will *never* be broad enough to snuff out a reasonable expectation of privacy," it expressed "doubt that will be the case in most situations." *Id.* at 286, 287. Google's TOS here is not categorically different from the subscriber agreement in *Warshak*, which "contractually reserved the right to access Warshak's emails for certain purposes." *Id.* at 286. In particular, Google's monitoring for policy violations and illegal activity does not place it beyond the reasonable expectation of privacy found by the Sixth Circuit. Nor is Google's TOS categorically different from the policy at issue in *Heckenkamp*,

which stated that the university could access private computers connected to the school network "where essential to . . . protect the integrity of the University and the rights and property of the state." 482 F.3d at 1147. Google, too, states it may monitor to ensure that users comply with its policies, including prohibitions on illegal conduct. ER 82. But it also advises users: "But that does not necessarily mean that we review content, so please don't assume that we do." *Id*.

Since this Court decided *Heckenkamp*, society, technology, and the law have evolved. Widespread adoption of email and other electronic communications hosted by third party service providers has led to a societal recognition that these materials are extremely private. That recognition goes hand-in-hand with the longstanding possessory interest people have in their email messages, as well as the growing number of statutes that seek to manage property rights in intangible data. Influenced by this trend, the Supreme Court has rejected mechanical application of older Fourth Amendment rules to new technologies, including the claim that information in the hands of third party service providers has less Fourth Amendment protection than privately held letters. *Carpenter*, 138 S. Ct. 2206; *See also Riley*, 573 U.S. 373; *United States v. Jones*, 565 U.S. 400 (2012).

Should any court approve of the district court's reasoning, it would go against the prevailing legal authority and create an unworkable circuit split. It would mean the Fourth Amendment requires a warrant for access to the electronic

communications of people living in Kentucky, Michigan, Ohio, and Tennessee, but the government could skirt that requirement when it wanted to access the email correspondence of people living in Alaska, Arizona, California, Hawaii, Idaho, Montana, Nevada, Oregon, and Washington. Not only would this patchwork of legal protections be unfair to email users and contrary to well-established understandings of email privacy, it would be a challenge to implement for both law enforcement and for email service providers who operate across the entire United States. *See Riley*, 573 U.S. at 398 (Fourth Amendment favors "clear guidance to law enforcement through categorical rules").

## CONCLUSION

For the reasons above, the Court should decline to adopt either the district court's or the government's reasoning and either hold that Mr. Wilson had a reasonable expectation of privacy in his email account, or assume that is the case for the purpose of deciding this appeal.

Dated: March 28, 2019

By: /s/ *Jennifer Lynch*
Jennifer Lynch
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
jlynch@eff.org

*Counsel for Amicus Curiae Electronic Frontier Foundation*

/s/ *Jennifer Stisa Granick*
Jennifer Stisa Granick
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111-4805
(415) 343-0758

Brett Max Kaufman
Nathan Freed Wessler
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street
New York, NY 10004
(212) 549-2500

*Counsel for Amicus Curiae ACLU*

**CERTIFICATE OF COMPLIANCE WITH RULE 32(A)**

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

[ X ] this brief contains 5,811 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii), or

[ ] this brief uses a monospaced typeface and contains [less than 650] lines of text, 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:

[ X ] this brief has been prepared in a proportionally spaced typeface using [Microsoft Word 2010] in [14 point Times New Roman font], or

[ ] this brief has been prepared in a monospaced typeface using [name and version of word processing program] with [number of characters per inch and name of type style].

Dated: March 28, 2019

By: /s/ Jennifer Lynch
Jennifer Lynch

*Counsel for Amici Curiae*

## CERTIFICATE OF SERVICE

I hereby certify that I served the foregoing Brief of Amici Curiae, on counsel for all parties, electronically through the ECF System, on this 28th day of March, 2019.

Dated: March 28, 2019

By: /s/ Jennifer Lynch
Jennifer Lynch
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
jlynch@eff.org

*Counsel for Amici Curiae*