JENNIFER LYNCH (SBN 240701)
jlynch@eff.org
ANDREW CROCKER (SBN 291596)
andrew@eff.org
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Fax: (415) 436-9993

Counsel for Amicus Curiae Electronic Frontier Foundation

Additional Counsel Listed on Following Page

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

UNITED STATES OF AMERICA, *Plaintiff,* v. JOHNNY RAY WOLFENBARGER, *Defendant.*	Case No. 5:16-cr-00519-LHK-1 **[PROPOSED] BRIEF OF AMICI CURIAE ELECTRONIC FRONTIER FOUNDATION, AMERICAN CIVIL LIBERTIES UNION, AND AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA IN SUPPORT OF DEFENDANT'S REQUEST FOR LEAVE TO FILE MOTION FOR RECONSIDERATION** Hon. Lucy H. Koh

ADDITIONAL COUNSEL:

JENNIFER STISA GRANICK (SBN 168423)
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

Counsel for Amicus Curiae American Civil Liberties Union

JACOB A. SNOW (SBN 270988)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111
(415) 621-2493

Counsel for Amicus Curiae American Civil Liberties Union Foundation of Northern California

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Constitutional Provisions

Legislative Materials

Other Authorities

STATEMENT OF INTEREST

The Electronic Frontier Foundation ("EFF") is a member-supported, non-profit civil liberties organization that works to protect free speech and privacy in the digital world. Founded in 1990, EFF has over 30,000 active donors and dues-paying members across the United States. EFF regularly participates as amicus in cases addressing the Fourth Amendment and its application to new technologies. *See, e.g., Carpenter v. United States*, 137 S. Ct. 2211 (2017); *Riley v. California*, 134 S. Ct. 2473 (2014); *City of Ontario v. Quon*, 560 U.S. 746 (2010); *United States v. Wilson*, No. 18-50440 (9th Cir.); *United States v. Ackerman*, No. 27-3238 (10th Cir.); *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). EFF is especially interested in the outcome of this case, given its past participation in cases like *Wilson, Ackerman* and *Warshak*.

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. The ACLU of Northern California is a state affiliate of the national ACLU. Since its founding in 1920, the ACLU has frequently 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

Amici write to urge the Court to reconsider its holding that individuals lack a reasonable expectation of privacy in certain content in their email accounts maintained by third-party providers who reserve the right to monitor and access the accounts' contents. The Fourth Amendment protects the contents of email because it "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); *see also United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2008). 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

communications and 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, this Court determined that, because Defendant "agreed" to his email service provider's terms of service ("TOS") stating that the provider may monitor or analyze his account for illegal or unwanted behavior, he lost his reasonable expectation of privacy in the images stored in his account. ECF No. 207 at 18, 20. However, there is no principled way to constrain the Court's holding to the eight contraband images; its analysis would instead apply to any and all emails, files, and attachments maintained with the service provider, in this case Yahoo, one of the largest email providers in the United States. The Court's holding would mean that a private company's TOS trumps Fourth Amendment protections for *all* content maintained with the provider, and for all users of that email service—perhaps hundreds of thousands, or even millions of people.[1] This is inconsistent with public expectations, well-recognized Fourth Amendment case law, and Supreme Court dicta. If this Court lets its holding stand, it would undermine fundamental privacy protections in communication media used by nearly all Americans.

The Court found that specific language in Yahoo's TOS allowing it to monitor users' content and remove it if it was "unlawful" or otherwise violated the TOS defeated Wolfenbarger'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). Under the Court's rationale, 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, the Court's approach could not be cabined

[1] Litmus, *Email Client Market Share* (September 2019), https://emailclientmarketshare.com/.

to child pornography cases. From a Fourth Amendment standpoint, there is no difference between the privacy interests versus the government in the eight image files that Yahoo forwarded to NCMEC and which a law enforcement officer reviewed, and the rest of Mr. Wolfenbarger's account. If Yahoo's TOS alone defeated Mr. Wolfenbarger's expectation privacy in these images, it would necessarily defeat it in the entire account. This would be contrary to *Warshak* and to Supreme Court dicta in *Carpenter*.

Amici respectfully urge this Court to reconsider its holding and make clear that a company's TOS, alone, does not defeat users' reasonable expectations of privacy in their email and uploaded files, even if their email contains contraband.

ARGUMENT

I. Courts Widely Recognize Fourth Amendment Protections for Electronic Communications and Documents Stored Online.

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.[2]

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*

[2] 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.

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, JK-15-029*, 828 F.3d 1083, 1090 (9th Cir. 2016).

For these reasons, in *Carpenter* every Justice of the Supreme Court cited *Warshak* and 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 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) (Just because you entrust your data—in some cases, your modern-day papers and effects—to a third party may not mean you lose any Fourth Amendment interest in its contents . . . few doubt that e-mail should be treated much like the traditional mail it has largely supplanted").

Since *Warshak*, all of the major electronic communications service providers, including Yahoo, require a warrant before turning over the contents of their users' accounts to the government.[3] And it has been Department of Justice policy since at least 2013 to seek warrants to

[3] *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").

access the contents of online messages.[4]

II. Neither a Service Provider's Ability to Monitor Its Users' Accounts Nor Its TOS Defeats its Users' Reasonable Expectations of Privacy in Their Email or Digital Papers.

The Court looked to Yahoo's terms of service to conclude that Mr. Wolfenbarger—and by extension any Yahoo email user—cannot have a reasonable expectation of privacy in contraband files uploaded to a Yahoo email account because the TOS advised him that it could monitor user accounts for violations of its policies and illegal conduct. ECF No. 207 at 17-19. However, while a private contract like Yahoo's TOS may govern the provider's relationship with the user, it cannot vitiate the user's Fourth Amendment rights vis à vis the government.

A. A Service Provider's Ability to Access Communications Does Not Defeat its Users' Reasonable Expectation of Privacy.

Individuals enjoy an expectation of privacy in their communications even though someone else may facilitate the sending and receiving of those communications. That is because merely entrusting "papers" and "effects" to an intermediary does not defeat the reasonable expectation that the contents of the materials will remain private. *Smith v. Maryland*, 442 U.S. 735, 741 (1979) (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, 648 (9th Cir. 1967)).

As the Sixth Circuit recognized in *Warshak*, Internet service providers ("ISPs") are the

---

[4] *See* H.R. Rep. No. 114-528, at 9 (April 26, 2016) (noting, "[s]oon after the [*Warshak*] decision, the Department of Justice began using warrants for email in all criminal cases. That practice became Department policy in 2013.").

"functional equivalent" of post offices or phone companies; they make "email 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 an ISP 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.

The Court's holding in this case—that the defendant lacks a reasonable expectation of privacy in the contents of his email stored with and accessible by Yahoo—runs counter to the reasoning in the cases cited above. It also 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.

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

B. TOS 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 reserved the right to monitor these records for limited purposes through its TOS. 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. These terms, with their reservations of rights, are almost never negotiated, and users have no choice but to click "I agree" just to engage in activities that are fundamental to modern life. *Riley*, 573 U.S. at 385.

Users' Fourth Amendment-protected expectations of privacy are not upended when third-

party providers give notice that they may exercise their 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 that users who agreed to this policy had 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 merely to protect their business from objectionable conduct or content.[5] But this Court's 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 by reserving the right to access user accounts and report violations to law enforcement, it would necessarily vitiate its users' expectations of privacy and thereby leave 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.[6]

The Supreme Court recently rejected the argument that Fourth Amendment rights can be determined by private form contracts in *United States v. Byrd*, 138 S. Ct. 1518 (2018). In *Byrd*, the police stopped and searched a rental car driven by someone who was not on the rental agreement but was given permission to drive by the renter. *Id.* at 1524. 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

---

[5] Providers' TOS almost universally allow them to monitor for certain purposes. *See, e.g., Gmail Program Policies*, https://www.google.com/gmail/about/policy/; docs.microsoft.com - Terms of Use, https://docs.microsoft.com/en-us/legal/termsofuse.

[6] Allowing the Court's ruling to stand would also 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/.

the rental agreement. *Id.* at 1529. 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. *Id.* 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.* 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.

Byrd is only the most recent example in a line of cases where courts have declined to find private contracts dispositive of individuals' expectations of privacy. These cases are consistent with the Supreme Court's explanation "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). In *Smith*, for example, the 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*, the Ninth 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).

The cases relied on by this Court in reaching its holding are inapposite or distinguishable. The Court cited to *United States v. Heckenkamp*, 482 F.3d 1142 (9th Cir. 2007), to suggest that there may be some terms that can obviate a reasonable expectation of privacy. However, the Ninth Circuit held in *Heckenkamp* that a university policy advising students that administrators might access network-attached computers in limited circumstances to protect the university's systems did

not defeat the student's reasonable expectation of privacy in his computer. Although the court suggested that a different policy advising students that their network traffic "is not confidential and that the systems administrators may monitor communications transmitted by the user" might reduce privacy expectations, that discussion was dicta. *Id.* at 1147 (noting, "[i]n the instant case, there was no announced monitoring policy on the network.")

Although *Heckenkamp* and even *Warshak* leave open the hypothetical possibility that courts could reach a different conclusion about TOS monitoring policies under some future and unknown set of facts, this case does not present those facts. *See Warshak*, 631 F.3d at 286, 287 ("[W]e are unwilling to hold that a subscriber agreement will *never* be broad enough to snuff out a reasonable expectation of privacy . . . we doubt that will be the case in most situations."). Yahoo'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, Yahoo'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 Yahoo'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. Yahoo, too, states it *may* monitor to ensure that users comply with its policies, including prohibitions on illegal conduct, but it does not claim to actively monitor all user content. ECF No. 188-1 at 8.

Heckenkamp is not persuasive in this case for two additional reasons. First, the search occurred in a university setting, which presents a different kind of relationship than that between a user and their ISP. Second, three years after *Heckenkamp*, the Supreme Court decided *Quon*, in which it explicitly refrained from finding that a broad monitoring policy would vitiate the defendant city employee's reasonable expectation of privacy in text message he sent via his employer's pager. *Id.* at 758 (policy stated that "'[u]sers should have no expectation of privacy or confidentiality when using' City computers"). Instead, the Court said it "must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer," and decided the case on narrower

grounds. *Id.* at 759.

This Court also relied on two district court cases, but neither support the Court's conclusions. ECF No. 207 at 19 (citing *United States v. Wilson*, 2017 WL 2733879 (S.D. Cal. June 26, 2017); *United States v. Viramontes*, 16-CR-508-EMC, ECF No. 62 (N.D Cal. Nov. 14, 2017)). First, the portion of *Wilson* relied on by this Court is dicta. 2017 WL 2733879, at *20 (S.D. Cal. June 26, 2017) ("The Court's resolution of the instant motion to suppress does not depend upon the finding that Defendant lacked an expectation of privacy in the four child pornography files he uploaded to his Google email account."). Further, *Wilson* is currently on appeal to the Ninth Circuit, and the government has not defended this dicta on appeal. *United States v. Wilson*, Dkt. No. 43, No. 18-50440 (9th Cir.) (argument set for November 2019). Second, Judge Chen's conclusion in *United States v. Viramontes*—that the defendant lacked an expectation of privacy in contraband files uploaded to his Dropbox account—was not premised on a violation of Dropbox's TOS. 16-CR-508-EMC (redacted version available at ECF No. 79 (March 13, 2018)). Rather, the court found that the defendant had chosen a Dropbox privacy setting that made the files publicly accessible, so they were "without Fourth Amendment protection." *See Viramontes*, ECF No. 79 at 10-11 (redacted public order denying motion to dismiss). The court's analysis of Dropbox's TOS was limited to an analytically distinct issue: whether Viramontes consented to search by *Dropbox* (not the government), which the court held to be a private actor. *Id.*

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

III. The Court's Reasoning Could Leave All Email Messages and Stored Content, Not Just Contraband Files, Unprotected by the Fourth Amendment.

Reconsideration of the Court's holding is additionally necessary because its reasoning cannot be cabined solely to contraband images uploaded to a third-party email account. In light of

how Yahoo and other providers' TOS are written, that would be a distinction without a difference. Yahoo advises its users that it may monitor or analyze their entire account. ECF No. 188-1 at 10. If, as the Court held, that admonition defeats the user's expectation of privacy, it would do so for the entire contents of a user's account. Nor does it matter that, when conducting this account monitoring, some files in that account are determined to be contraband after the fact. 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.at 1524 (reasonable expectation of privacy in rental car containing heroin); *Jacobsen*, 466 U.S. at 114 (reasonable expectation of privacy in parcel containing cocaine); *Owens*, 782 F.2d at 150 (reasonable expectation of privacy in hotel room containing cocaine). The same is true with Mr. Wolfenbarger's Yahoo 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. The Court's Reasoning Would Reinstate the Third-Party Doctrine for Email, Disregarding Precedent from Appellate Courts.

Although the Court did not explicitly cite to the "third party doctrine," it implicitly ruled the third party doctrine applies to email and digital "papers" stored online by holding the defendant lacks a reasonable expectation of privacy in content he entrusted to Yahoo, his third party email provider. This runs counter to the public's expectations that their email communications are private and is inconsistent with appellate and Supreme Court precedent.

The Court held that Defendant "acknowledged" that Yahoo could access and search content in his account and that this "functions as consent" to a search. ECF No. 207 at 19. This is essentially the same analysis articulated by the Supreme Court when it held in *Smith* that phone users have no reasonable expectation of privacy in the numbers they dial on their phone because those numbers are shared with a third party phone company. *See Smith*, 442 U.S. at 743 (phone users "know" they convey their dialed numbers to the phone company). It is also similar to the

reasoning in *United States v. Miller* that a bank "depositor takes the risk, in revealing his affairs to [the third party bank], that the information will be conveyed by that person to the Government." 425 U.S. 435, 443 (1976).

However, ruling that email users have no expectation of privacy in their email because they knowingly assumed the risk that the ISP could turn the contents of their email over to the government runs counter to *Warshak* and *Carpenter* and to the public's understanding of that email communications are protected. *See Warshak*, 631 F.3d at 285, 287 (distinguishing *Smith*, 442 U.S. at 746); Section II.A., *supra*. It also runs counter to the practices of major internet companies and the government, which regularly obtains a warrant for email.[7] In other words, the third party doctrine does not apply to the contents of email accounts. Should this court find that a service provider could, through its TOS, unilaterally abrogate its users' 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.

CONCLUSION

Since the decisions in *Warshak*, *Heckenkamp*, and *Quon*, the near-universal adoption of email and other electronic communications hosted by third party service providers has only deepened the longstanding societal recognition that these materials are extremely private. 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. 2222; *see also Riley*, 573 U.S. at 395; *United States v. Jones*, 565 U.S. 400, 430 (2012). Users' expectations of privacy in electronic communications maintained by ISPs are also bolstered by the recent decision in *Byrd*, in which the Supreme Court refused to delegate the power to delineate Fourth Amendment protections to private contracts of adhesion.

[7] *See* notes 5,6, *supra*.

In light of this prevailing legal authority and for the reasons stated above, amici respectfully request the Court reconsider its TOS holding.

Dated: November 1, 2019

By: /s/ *Jennifer Lynch*
Jennifer Lynch
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (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 American Civil Liberties Union

/s/ *Jacob A. Snow*
Jacob A. Snow
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111
(415) 621-2493

Counsel for Amicus Curiae American Civil Liberties Union Foundation of Northern California

CERTIFICATE OF SERVICE

I hereby certify that on November 1, 2019, I submitted for filing the foregoing with the Clerk of the Court and caused to be served by U.S. Mail, postage thereon fully prepaid, a true and correct copy of the foregoing on:

Severa Keith
Office of the Federal Public Defender
San Jose Office
55 South Market Street, Suite 820
San Jose, CA 95113

Graham E. Archer
Federal Public Defender
13th Floor Federal Building - Suite 1350N
1301 Clay Street
Oakland, CA 94612

Counsel for Defendant John Wolfenbarger

Marissa Harris
U.S. Attorneys Office
Northern District California
150 Almaden Blvd., Ste. 900
San Jose, CA 95113

Counsel for Plaintiff U.S.A.

Alexandra Whitworth
Bryan Cave Leighton Paisner LLP
Three Embarcadero Center, 7th Floor
San Francisco, CA 94111-4070

Counsel for Movant The National Center for Missing and Exploited Children

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct. Dated this 1st day of November, 2019.

/s/ Jennifer Lynch
Jennifer Lynch

ADDITIONAL COUNSEL:

JENNIFER STISA GRANICK (SBN 168423)
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

Counsel for Amicus Curiae American Civil Liberties Union

JACOB A. SNOW (SBN 270988)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111
(415) 621-2493

Counsel for Amicus Curiae American Civil Liberties Union Foundation of Northern California

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Constitutional Provisions

Legislative Materials

Other Authorities

STATEMENT OF INTEREST

The Electronic Frontier Foundation ("EFF") is a member-supported, non-profit civil liberties organization that works to protect free speech and privacy in the digital world. Founded in 1990, EFF has over 30,000 active donors and dues-paying members across the United States. EFF regularly participates as amicus in cases addressing the Fourth Amendment and its application to new technologies. *See, e.g., Carpenter v. United States*, 137 S. Ct. 2211 (2017); *Riley v. California*, 134 S. Ct. 2473 (2014); *City of Ontario v. Quon*, 560 U.S. 746 (2010); *United States v. Wilson*, No. 18-50440 (9th Cir.); *United States v. Ackerman*, No. 27-3238 (10th Cir.); *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). EFF is especially interested in the outcome of this case, given its past participation in cases like *Wilson, Ackerman* and *Warshak.*

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. The ACLU of Northern California is a state affiliate of the national ACLU. Since its founding in 1920, the ACLU has frequently 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

Amici write to urge the Court to reconsider its holding that individuals lack a reasonable expectation of privacy in certain content in their email accounts maintained by third-party providers who reserve the right to monitor and access the accounts' contents. The Fourth Amendment protects the contents of email because it "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); *see also United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2008). 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

communications and 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, this Court determined that, because Defendant "agreed" to his email service provider's terms of service ("TOS") stating that the provider may monitor or analyze his account for illegal or unwanted behavior, he lost his reasonable expectation of privacy in the images stored in his account. ECF No. 207 at 18, 20. However, there is no principled way to constrain the Court's holding to the eight contraband images; its analysis would instead apply to any and all emails, files, and attachments maintained with the service provider, in this case Yahoo, one of the largest email providers in the United States. The Court's holding would mean that a private company's TOS trumps Fourth Amendment protections for *all* content maintained with the provider, and for all users of that email service—perhaps hundreds of thousands, or even millions of people.[1] This is inconsistent with public expectations, well-recognized Fourth Amendment case law, and Supreme Court dicta. If this Court lets its holding stand, it would undermine fundamental privacy protections in communication media used by nearly all Americans.

The Court found that specific language in Yahoo's TOS allowing it to monitor users' content and remove it if it was "unlawful" or otherwise violated the TOS defeated Wolfenbarger'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). Under the Court's rationale, 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, the Court's approach could not be cabined

[1] Litmus, *Email Client Market Share* (September 2019), https://emailclientmarketshare.com/.

to child pornography cases. From a Fourth Amendment standpoint, there is no difference between the privacy interests versus the government in the eight image files that Yahoo forwarded to NCMEC and which a law enforcement officer reviewed, and the rest of Mr. Wolfenbarger's account. If Yahoo's TOS alone defeated Mr. Wolfenbarger's expectation privacy in these images, it would necessarily defeat it in the entire account. This would be contrary to *Warshak* and to Supreme Court dicta in *Carpenter*.

Amici respectfully urge this Court to reconsider its holding and make clear that a company's TOS, alone, does not defeat users' reasonable expectations of privacy in their email and uploaded files, even if their email contains contraband.

ARGUMENT

I. Courts Widely Recognize Fourth Amendment Protections for Electronic Communications and Documents Stored Online.

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.[2]

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*

[2] 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.

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, JK-15-029*, 828 F.3d 1083, 1090 (9th Cir. 2016).

For these reasons, in *Carpenter* every Justice of the Supreme Court cited *Warshak* and 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 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) (Just because you entrust your data—in some cases, your modern-day papers and effects—to a third party may not mean you lose any Fourth Amendment interest in its contents . . . few doubt that e-mail should be treated much like the traditional mail it has largely supplanted").

Since *Warshak*, all of the major electronic communications service providers, including Yahoo, require a warrant before turning over the contents of their users' accounts to the government.[3] And it has been Department of Justice policy since at least 2013 to seek warrants to

[3] *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").

access the contents of online messages.[4]

II. Neither a Service Provider's Ability to Monitor Its Users' Accounts Nor Its TOS Defeats its Users' Reasonable Expectations of Privacy in Their Email or Digital Papers.

The Court looked to Yahoo's terms of service to conclude that Mr. Wolfenbarger—and by extension any Yahoo email user—cannot have a reasonable expectation of privacy in contraband files uploaded to a Yahoo email account because the TOS advised him that it could monitor user accounts for violations of its policies and illegal conduct. ECF No. 207 at 17-19. However, while a private contract like Yahoo's TOS may govern the provider's relationship with the user, it cannot vitiate the user's Fourth Amendment rights vis à vis the government.

A. A Service Provider's Ability to Access Communications Does Not Defeat its Users' Reasonable Expectation of Privacy.

Individuals enjoy an expectation of privacy in their communications even though someone else may facilitate the sending and receiving of those communications. That is because merely entrusting "papers" and "effects" to an intermediary does not defeat the reasonable expectation that the contents of the materials will remain private. *Smith v. Maryland*, 442 U.S. 735, 741 (1979) (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, 648 (9th Cir. 1967)).

As the Sixth Circuit recognized in *Warshak*, Internet service providers ("ISPs") are the

[4] *See* H.R. Rep. No. 114-528, at 9 (April 26, 2016) (noting, "[s]oon after the [*Warshak*] decision, the Department of Justice began using warrants for email in all criminal cases. That practice became Department policy in 2013.").

"functional equivalent" of post offices or phone companies; they make "email 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 an ISP 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.

The Court's holding in this case—that the defendant lacks a reasonable expectation of privacy in the contents of his email stored with and accessible by Yahoo—runs counter to the reasoning in the cases cited above. It also 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.

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

B. TOS 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 reserved the right to monitor these records for limited purposes through its TOS. 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. These terms, with their reservations of rights, are almost never negotiated, and users have no choice but to click "I agree" just to engage in activities that are fundamental to modern life. *Riley*, 573 U.S. at 385.

Users' Fourth Amendment-protected expectations of privacy are not upended when third-

party providers give notice that they may exercise their 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 that users who agreed to this policy had 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 merely to protect their business from objectionable conduct or content.[5] But this Court's 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 by reserving the right to access user accounts and report violations to law enforcement, it would necessarily vitiate its users' expectations of privacy and thereby leave 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.[6]

The Supreme Court recently rejected the argument that Fourth Amendment rights can be determined by private form contracts in *United States v. Byrd*, 138 S. Ct. 1518 (2018). In *Byrd*, the police stopped and searched a rental car driven by someone who was not on the rental agreement but was given permission to drive by the renter. *Id.* at 1524. 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

---

[5] Providers' TOS almost universally allow them to monitor for certain purposes. *See, e.g., Gmail Program Policies*, https://www.google.com/gmail/about/policy/; docs.microsoft.com - Terms of Use, https://docs.microsoft.com/en-us/legal/termsofuse.

[6] Allowing the Court's ruling to stand would also 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/.

the rental agreement. *Id.* at 1529. 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. *Id.* 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.* 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.

Byrd is only the most recent example in a line of cases where courts have declined to find private contracts dispositive of individuals' expectations of privacy. These cases are consistent with the Supreme Court's explanation "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). In *Smith*, for example, the 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*, the Ninth 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).

The cases relied on by this Court in reaching its holding are inapposite or distinguishable. The Court cited to *United States v. Heckenkamp*, 482 F.3d 1142 (9th Cir. 2007), to suggest that there may be some terms that can obviate a reasonable expectation of privacy. However, the Ninth Circuit held in *Heckenkamp* that a university policy advising students that administrators might access network-attached computers in limited circumstances to protect the university's systems did

not defeat the student's reasonable expectation of privacy in his computer. Although the court suggested that a different policy advising students that their network traffic "is not confidential and that the systems administrators may monitor communications transmitted by the user" might reduce privacy expectations, that discussion was dicta. *Id.* at 1147 (noting, "[i]n the instant case, there was no announced monitoring policy on the network.")

Although *Heckenkamp* and even *Warshak* leave open the hypothetical possibility that courts could reach a different conclusion about TOS monitoring policies under some future and unknown set of facts, this case does not present those facts. *See Warshak*, 631 F.3d at 286, 287 ("[W]e are unwilling to hold that a subscriber agreement will *never* be broad enough to snuff out a reasonable expectation of privacy . . . we doubt that will be the case in most situations."). Yahoo'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, Yahoo'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 Yahoo'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. Yahoo, too, states it *may* monitor to ensure that users comply with its policies, including prohibitions on illegal conduct, but it does not claim to actively monitor all user content. ECF No. 188-1 at 8.

Heckenkamp is not persuasive in this case for two additional reasons. First, the search occurred in a university setting, which presents a different kind of relationship than that between a user and their ISP. Second, three years after *Heckenkamp*, the Supreme Court decided *Quon*, in which it explicitly refrained from finding that a broad monitoring policy would vitiate the defendant city employee's reasonable expectation of privacy in text message he sent via his employer's pager. *Id.* at 758 (policy stated that "'[u]sers should have no expectation of privacy or confidentiality when using' City computers"). Instead, the Court said it "must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer," and decided the case on narrower

grounds. *Id.* at 759.

This Court also relied on two district court cases, but neither support the Court's conclusions. ECF No. 207 at 19 (citing *United States v. Wilson*, 2017 WL 2733879 (S.D. Cal. June 26, 2017); *United States v. Viramontes*, 16-CR-508-EMC, ECF No. 62 (N.D Cal. Nov. 14, 2017)). First, the portion of *Wilson* relied on by this Court is dicta. 2017 WL 2733879, at *20 (S.D. Cal. June 26, 2017) ("The Court's resolution of the instant motion to suppress does not depend upon the finding that Defendant lacked an expectation of privacy in the four child pornography files he uploaded to his Google email account."). Further, *Wilson* is currently on appeal to the Ninth Circuit, and the government has not defended this dicta on appeal. *United States v. Wilson*, Dkt. No. 43, No. 18-50440 (9th Cir.) (argument set for November 2019). Second, Judge Chen's conclusion in *United States v. Viramontes*—that the defendant lacked an expectation of privacy in contraband files uploaded to his Dropbox account—was not premised on a violation of Dropbox's TOS. 16-CR-508-EMC (redacted version available at ECF No. 79 (March 13, 2018)). Rather, the court found that the defendant had chosen a Dropbox privacy setting that made the files publicly accessible, so they were "without Fourth Amendment protection." *See Viramontes*, ECF No. 79 at 10-11 (redacted public order denying motion to dismiss). The court's analysis of Dropbox's TOS was limited to an analytically distinct issue: whether Viramontes consented to search by *Dropbox* (not the government), which the court held to be a private actor. *Id.*

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

III. The Court's Reasoning Could Leave All Email Messages and Stored Content, Not Just Contraband Files, Unprotected by the Fourth Amendment.

Reconsideration of the Court's holding is additionally necessary because its reasoning cannot be cabined solely to contraband images uploaded to a third-party email account. In light of

how Yahoo and other providers' TOS are written, that would be a distinction without a difference. Yahoo advises its users that it may monitor or analyze their entire account. ECF No. 188-1 at 10. If, as the Court held, that admonition defeats the user's expectation of privacy, it would do so for the entire contents of a user's account. Nor does it matter that, when conducting this account monitoring, some files in that account are determined to be contraband after the fact. 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.at 1524 (reasonable expectation of privacy in rental car containing heroin); *Jacobsen*, 466 U.S. at 114 (reasonable expectation of privacy in parcel containing cocaine); *Owens*, 782 F.2d at 150 (reasonable expectation of privacy in hotel room containing cocaine). The same is true with Mr. Wolfenbarger's Yahoo 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. The Court's Reasoning Would Reinstate the Third-Party Doctrine for Email, Disregarding Precedent from Appellate Courts.

Although the Court did not explicitly cite to the "third party doctrine," it implicitly ruled the third party doctrine applies to email and digital "papers" stored online by holding the defendant lacks a reasonable expectation of privacy in content he entrusted to Yahoo, his third party email provider. This runs counter to the public's expectations that their email communications are private and is inconsistent with appellate and Supreme Court precedent.

The Court held that Defendant "acknowledged" that Yahoo could access and search content in his account and that this "functions as consent" to a search. ECF No. 207 at 19. This is essentially the same analysis articulated by the Supreme Court when it held in *Smith* that phone users have no reasonable expectation of privacy in the numbers they dial on their phone because those numbers are shared with a third party phone company. *See Smith*, 442 U.S. at 743 (phone users "know" they convey their dialed numbers to the phone company). It is also similar to the

reasoning in *United States v. Miller* that a bank "depositor takes the risk, in revealing his affairs to [the third party bank], that the information will be conveyed by that person to the Government." 425 U.S. 435, 443 (1976).

However, ruling that email users have no expectation of privacy in their email because they knowingly assumed the risk that the ISP could turn the contents of their email over to the government runs counter to *Warshak* and *Carpenter* and to the public's understanding of that email communications are protected. *See Warshak*, 631 F.3d at 285, 287 (distinguishing *Smith*, 442 U.S. at 746); Section II.A., *supra*. It also runs counter to the practices of major internet companies and the government, which regularly obtains a warrant for email.[7] In other words, the third party doctrine does not apply to the contents of email accounts. Should this court find that a service provider could, through its TOS, unilaterally abrogate its users' 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.

CONCLUSION

Since the decisions in *Warshak*, *Heckenkamp*, and *Quon*, the near-universal adoption of email and other electronic communications hosted by third party service providers has only deepened the longstanding societal recognition that these materials are extremely private. 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. 2222; *see also Riley*, 573 U.S. at 395; *United States v. Jones*, 565 U.S. 400, 430 (2012). Users' expectations of privacy in electronic communications maintained by ISPs are also bolstered by the recent decision in *Byrd*, in which the Supreme Court refused to delegate the power to delineate Fourth Amendment protections to private contracts of adhesion.

[7] *See* notes 5,6, *supra*.

In light of this prevailing legal authority and for the reasons stated above, amici respectfully request the Court reconsider its TOS holding.

Dated: November 1, 2019

By: /s/ *Jennifer Lynch*
Jennifer Lynch
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (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 American Civil Liberties Union

/s/ *Jacob A. Snow*
Jacob A. Snow
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111
(415) 621-2493

Counsel for Amicus Curiae American Civil Liberties Union Foundation of Northern California

CERTIFICATE OF SERVICE

I hereby certify that on November 1, 2019, I submitted for filing the foregoing with the Clerk of the Court and caused to be served by U.S. Mail, postage thereon fully prepaid, a true and correct copy of the foregoing on:

Severa Keith
Office of the Federal Public Defender
San Jose Office
55 South Market Street, Suite 820
San Jose, CA 95113

Graham E. Archer
Federal Public Defender
13th Floor Federal Building - Suite 1350N
1301 Clay Street
Oakland, CA 94612

Counsel for Defendant John Wolfenbarger

Marissa Harris
U.S. Attorneys Office
Northern District California
150 Almaden Blvd., Ste. 900
San Jose, CA 95113

Counsel for Plaintiff U.S.A.

Alexandra Whitworth
Bryan Cave Leighton Paisner LLP
Three Embarcadero Center, 7th Floor
San Francisco, CA 94111-4070

Counsel for Movant The National Center for Missing and Exploited Children

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct. Dated this 1st day of November, 2019.

/s/ Jennifer Lynch
Jennifer Lynch