NO. 17-3238

IN THE UNITED STATES COURT OF APPEALS
FOR THE TENTH CIRCUIT

UNITED STATES OF AMERICA,

PLAINTIFF-APPELLEE,

V.

WALTER E. ACKERMAN

DEFENDANT-APPELLANT

On Appeal from the United States District Court
for the District of Kansas – Wichita
No. 13-cr-10176-EFM
The Honorable Eric F. Melgren, United States District Court Judge

BRIEF OF AMICI CURIAE ELECTRONIC FRONTIER FOUNDATION, BRENNAN CENTER FOR JUSTICE, CENTER FOR DEMOCRACY AND TECHNOLOGY, AND NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS IN SUPPORT OF DEFENDANT-APPELLANT AND REVERSAL

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

Counsel for Amici Curiae Electronic Frontier Foundation, Brennan Center for Justice at NYU School of Law, and Center for Democracy and Technology

Barbara E. Bergman
Co-chair, NACDL Amicus Committee
James E. Rogers College of Law
The University of Arizona
1201 E. Speedway Drive
Tucson, AZ 85721
(505) 301-7547
bbergman@email.arizona.edu

Counsel for Amicus Curiae
National Association of
Criminal Defense Lawyers

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

Legislative Authorities

Constitutional Provisions

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,* 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. Workman*, 863 F.3d 1313 (10th Cir. 2017); *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 *Warshak* and its extensive work to ensure Fourth Amendment protection for electronic communications.

Amicus curiae the Brennan Center for Justice at NYU School of Law is a non-partisan public policy and law institute focused on fundamental issues of

[1] Pursuant to Federal Rule of Appellate Procedure Rule 29(a)(2), amici represent that all parties have consented to the filing of this brief. This brief does not purport to represent the position of NYU School of Law.

democracy and justice. The Center's Liberty and National Security (LNS) Program uses innovative policy recommendations, litigation, and public advocacy to advance effective national security policies that respect the rule of law and constitutional values. The LNS Program is particularly concerned with domestic surveillance and related law enforcement policies, including the dragnet collection of Americans' communications and personal data, and the concomitant effects on First and Fourth Amendment freedoms.

Amicus curiae the Center for Democracy & Technology (CDT) is a non-profit, public interest organization focused on privacy and other civil liberties issues affecting the Internet, other communications networks, and associated technologies. CDT represents the public's interest in an open Internet and promotes the constitutional and democratic values of free expression, privacy, and individual liberty. CDT has participated as amicus curiae in cases before the Supreme Court involving the application of the Fourth Amendment to new technologies, including *Carpenter v. United States*, 137 S. Ct. 2211 (2017); *Riley v. Californi*a, 134 S. Ct. 2473 (2014); *United States v. Jones*, 565 U.S. 400 (2012); and *City of Ontario v. Quon*, 560 U.S. 746 (2010).

Amicus curiae the National Association of Criminal Defense Lawyers (NACDL) is a nonprofit voluntary professional bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those

accused of crime or misconduct. NACDL was founded in 1958. It has a nationwide membership of many thousands of direct members, and up to 40,000 with affiliates. NACDL's members include private criminal defense lawyers, public defenders, military defense counsel, law professors, and judges. NACDL is the only nationwide professional bar association for public defenders and private criminal defense lawyers. NACDL is dedicated to advancing the proper, efficient, and just administration of justice. NACDL files numerous amicus briefs each year in the U.S. Supreme Court and other federal and state courts, seeking to provide amicus assistance in cases that present issues of broad importance to criminal defendants, criminal defense lawyers, and the criminal justice system as a whole. This case presents issues of great importance to NACDL, including the Fourth Amendment rights safeguarding individuals' reasonable expectations of privacy in their emails held in accounts operated by third party providers.

INTRODUCTION

The Fourth Amendment protects the contents of email 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). Following *Warshak*, courts have routinely held that individuals have a reasonable expectation of privacy in their email held in accounts operated by third party providers, even when those providers can access emails pursuant to contractual terms of service. Yet the district court below held that when an email service provider terminates a user's account pursuant to its terms of service, it extinguishes the user's expectation of privacy. This holding is inconsistent with well-recognized Fourth Amendment case law, and it threatens to undermine fundamental privacy protections in the communication mediums used by nearly all Americans.

The district court's holding, if upheld, could have broad impact. Although this case involves child pornography, the lower court's holding is in no way limited to child pornography cases or even to those involving serious crimes. Instead, under the court's rationale, Fourth Amendment protections rise and fall depending on form contracts written by private parties and the unilateral actions taken pursuant to those contracts. Neither can the district court's holding be cabined to a single email as the court suggested. Instead, under the court's rationale, a service provider's unilateral actions could vitiate any email user's

reasonable expectation of privacy in their entire account—likely comprising thousands of emails describing sensitive and intimate details of that user's life. This Court should not allow such a sweeping invalidation of constitutional rights to stand.

ARGUMENT

I. THE DISTRICT COURT'S OPINION UNDERMINES WIDELY RECOGNIZED FOURTH AMENDMENT PROTECTIONS FOR EMAIL.

A. The Expectation of Privacy in Email is Reasonable and Well Established.

Individuals have a reasonable expectation of privacy in their communications, including in email hosted by third-party providers. *Warshak*, 631 F.3d at 285-86. Like letters and phone calls, email "implicates the Fourth Amendment's specific guarantee of the people's right to be secure in their 'papers[.]'" *United States v. Cotterman*, 709 F.3d 952, 964 (9th Cir. 2013) (en banc) (citing U.S. Const. amend. IV); *Katz v. United States*, 389 U.S. 347, 352 (1967); *United States v. Jacobsen*, 466 U.S. 109, 114 (1984) ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy[.]").

For many if not most people, email and other electronic communications have in recent years far surpassed or even entirely replaced letters and phone calls as a means of communication. Whereas in the past people would have

communicated personal and private information via letter or over the phone, today we use electronic communications to "send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button." *Warshak*, 631 F.3d at 284. Email and other electronic communications have become so pervasive that many would "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 single letter, but years or decades worth of communications. Service providers offer many gigabytes of storage for free,[2] so people have little incentive to delete email. One 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

[2] For example, Google offers its email users 15 gigabytes of storage—the equivalent of about 150 yards of books on a shelf. Google Drive, https://www.google.com/drive/; Joel Lee, *Memory Sizes Explained – Gigabytes, Terabytes & Petabytes in Layman's Terms*, MakeUseOf.com (Aug. 14, 2012), https://www.makeuseof.com/tag/memory-sizes-gigabytes-terabytes-petabytes/. Yahoo offers one terabyte of storage, and AOL has offered unlimited storage. Yahoo Help, *Identify the percentage of storage used in Yahoo Mail*, https://help.yahoo.com/kb/SLN22068.html; David Eitelbach, *Yahoo Mail vs. Outlook.com vs. Gmail vs. AOL Mail*, Laptopmag.com (Sept. 19, 2014), https://www.laptopmag.com/articles/best-free-email-service.

their inbox.[3] Like the modern cellphone, email accounts today can contain "a digital record of nearly every aspect of [people's] lives—from the mundane to the intimate." *Riley v. California*, 134 S. Ct. 2473, 2490 (2014). As this Court recognized in its previous opinion, email is "a form of communication capable of storing all sorts of private and personal details, from correspondence to images, video or audio files, and so much more." *United States v. Ackerman*, 831 F.3d 1292, 1304 (10th Cir. 2016). "Account," the Sixth Circuit noted in *Warshak*, is a particularly "apt word for the conglomeration of stored messages that comprises an email account, as it provides an *account* of its owner's life." 631 F.3d at 284 (emphasis added).

For all these reasons, email users have a reasonable expectation of privacy in their emails. *Id.* at 288.[4] As such, the government must get a warrant to access them. *Id.* Since *Warshak* was decided, its holding has been adopted by every court to have squarely decided the question of whether the Fourth Amendment protects the contents of email held by an ISP.[5] Other courts have also recognized electronic

[3] 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.

[4] Indeed, in this case, the government has conceded the defendant had a reasonable expectation of privacy in his email before AOL terminated his account. *United States v. Ackerman,* No. 13–10176–01–EFM, 2017 WL 4890433, at *3 (D. Kan. Oct. 30, 2017).

[5] *See* Orin S. Kerr, The Next Generation Communications Privacy Act, 162 U. Pa. L. Rev. 373, 400 (2014); *see also, e.g., In re Applications for Search Warrants for*

communications are no different from traditional mail, and the Fourth Amendment protects the two equally. *See*, *e.g.*, *United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2007) (noting government surveillance of email is "conceptually indistinguishable from government surveillance of physical mail"); *Cotterman*, 709 F.3d at 964; *United States v. Mohamud*, 843 F.3d 420, 442 (9th Cir. 2016). It is also followed by all of the major electronic communications service providers, who require a warrant before turning over the contents of their users' communications to the government.[6] And it has been followed by the government,

---

Info. Associated with Target Email Address, Nos. 12–MJ–8119–DJW, 12–MJ–8191–DJW, 2012 WL 4383917, at *5 (D. Kan. Sep. 21, 2012) ("The Court finds the rationale set forth in *Warshak* persuasive and therefore holds that an individual has a reasonable expectation of privacy in emails or faxes stored with, sent to, or received through an electronic communications service provider."); *United States v. Ali*, 870 F. Supp. 2d 10, 39 n.39 (D.D.C. 2012) (recognizing a reasonable expectation of privacy in the content of emails). *See also Matter of Search of Info. Associated with [Redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.*, 13 F. Supp. 3d 145, 150 (D.D.C. 2014), *vacated sub nom*; *Matter of Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.*, 13 F. Supp. 3d 157 (D.D.C. 2014) (acknowledging *Warshak* and also holding emails turned over the government are "seized" for Fourth Amendment purposes); *State v. Hinton*, 280 P.3d 476, 483 (Wash. Ct. App. 2012) ("While *Warshak* does not aid Hinton, its comparison of e-mails with traditional forms of communication is helpful and we adopt it to hold that text messages deserve privacy protection similar to that provided for letters.").

[6] As of 2017, all major technology companies that store user content such as email in the United States require a warrant for law enforcement to access that content. *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

which, as in this case, has both conceded the reasonableness of defendants' expectations of privacy in their email and has regularly sought warrants to access it and other forms of electronic communications.[7]

B. The Ability of a Third Party Service Provider to Access Emails Does Not Defeat the User's Reasonable Expectation of Privacy.

Individuals enjoy an expectation of privacy in email despite the fact that third parties facilitate the sending and receiving of messages. That is because merely entrusting communications to an intermediary does not defeat the reasonable expectation that the contents of the communications 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. Likewise, since the Supreme Court's ruling in *Katz* in 1967, it has been "abundantly clear that telephone conversations . . . are fully protected by the Fourth and Fourteenth

---

(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").

[7] *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").

Amendments"—even though telephone companies have the capacity to monitor, listen in on, and record calls. *See Smith*, 442 U.S. at 746-47 (Stewart, J., dissenting) (citing *Katz*, 389 U.S. at 352). As *Warshak* recognized, third-party Internet service providers are the "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 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.

As the *Warshak* court noted, this finds further support "in the application of Fourth Amendment doctrine to rented space." *Id*. at 287. Tenants and hotel guests enjoy Fourth Amendment protection for their possessions stored in rented spaces, and a landlord or hotel employee's ability to enter the space does not diminish the renter's legitimate expectation of privacy. *See Stoner v. California*, 376 U.S. 483, 490 (1964); *Chapman v. United States*, 365 U.S. 610 (1961); *United States v. Owens*, 782 F.2d 146, 149 (10th Cir. 1986).

Given the cases above, Ackerman had a reasonable expectation of privacy in the contents of his emails stored with AOL, despite AOL's ability to access them.

II. AN EMAIL PROVIDER'S TERMS OF SERVICE SHOULD NOT DEFEAT A USER'S REASONABLE EXPECTATION OF PRIVACY IN EMAIL.

A. The District Court's Holding that AOL's TOS Extinguished Defendant's Reasonable Expectation of Privacy Is Inconsistent with Established Fourth Amendment Protections for Email.

Even though the government agreed that the defendant in this case initially had an expectation of privacy in his email stored by AOL, it claimed his expectation of privacy was extinguished when AOL terminated his account for violating its terms of service (TOS). *United States v. Ackerman,* No. 13–10176–01–EFM, 2017 WL 4890433, at *3 (D. Kan. Oct. 30, 2017). The district court agreed, holding that ISPs can unilaterally vitiate individuals' Fourth Amendment rights merely by terminating a user's account for a violation of a private contractual term. The court attempted to cabin its holding to the single email and four attachments at issue in this case, but its rationale would apply to every email in Ackerman's account. As such, the holding lacks internal logic and undermines basic Fourth Amendment protections for email.

This holding is illogical because either the defendant had a reasonable expectation of privacy in his email, as the government conceded, or AOL's TOS prevented him from ever forming an objectively reasonable expectation of privacy; both cannot be true simultaneously. According to the district court, the mere "*existence* of a TOS agreement diminishes a user's objectively reasonable

expectation of privacy." *Ackerman*, 2017 WL 4890433, at *4 (emphasis added). The court found AOL's TOS "alerted Defendant that he was not to participate or engage in illegal activity," and thus by its terms "limit[ed] Defendant's objectively reasonable expectation of privacy." *Id.* But if the mere existence of a TOS can limit users' expectations of privacy, the defendant could not have formed a reasonable expectation of privacy in any of his email in the first place. After all, the TOS applied to all of his email from the moment of account creation. *Id.* at *1.

Although the district court purported to draw the line at account termination, its reasoning does not depend on termination to extinguish an expectation of privacy, nor does the court's opinion explain why termination should have that effect. The court cited two district court cases to buttress its position, but neither of those cases turned on a provider's termination of a user's account to determine the user's expectation of privacy. *Ackerman*, 2017 WL 4890433, at *4 (citing *United States v. Stratton*, 229 F. Supp. 3d 1230, 1242 (D. Kan. 2017); *United States v. Wilson*, No. 3:15-cr-02838-GPC, 2017 WL 2733879, at *7 (S.D. Cal. June 26, 2017)). Instead, both cases stated (mistakenly) that providers' terms of service negated a user's expectation of privacy ab initio. *Stratton*, 229 F. Supp. 3d at 1242 (Sony PlayStation Network TOS entirely "prevented defendant from having a reasonable expectation of privacy in information he stored on his PS3 device"); *Wilson*, 2017 WL 2733879, at *7 (defendant had a reasonable expectation of

privacy in Google email account, but Google TOS rendered expectation of privacy in child pornography attachments unreasonable).

Further, the discussion of terms of service and reasonable expectation of privacy in both *Stratton* and *Wilson* is dicta, because both courts determined that the government had not gone further than the search first conducted by the providers and was therefore immunized by the "private search" doctrine. *Stratton*, 229 F. Supp. 3d at 1240; *Wilson*, 2017 WL 2733879, at *9-10. By contrast, this Court has already concluded that NCMEC exceeded AOL's search, so the private search doctrine does not immunize the government's actions here. *Ackerman*, 831 F.3d at 1305-06.

B. Fourth Amendment Protection Should Not Depend on Private Agreements Between Email Service Providers and Their Users.

The district court's opinion stands for the dangerous proposition that Fourth Amendment protections can be determined entirely by a private email provider's terms of service. This Court should decline to allow such private agreements to trump bedrock Fourth Amendment protections for private communications.

Terms of service provide a poor vehicle for determining an objective expectation of privacy. Fundamentally, they govern the relationship between the user and the provider, not the user and the government. These terms may reflect rights reserved by providers to protect their business from fraud or criminal

behavior, such as the specific provisions highlighted by the district court below as well as the *Stratton* and *Wilson* courts. *Ackerman*, 2017 WL 4890433, at *1, *4. But, as the Sixth Circuit pointed out in *Warshak*, a term of service granting the "right of access" or "the mere *ability* . . . to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy." 631 F.3d at 286-87 (emphasis original). If the reservation of such rights by a private party were enough to defeat an expectation of privacy, the Supreme Court in *Katz* could not have found that individuals have an expectation of privacy in their phone calls. *Id; see also Bubis v. United States*, 382 F.3d 607 (9th Cir. 1967) (telephone company could monitor calls to protect against illegal use of its facilities). A "telephone conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment. Yet, [the Supreme Court] squarely held that the user of even a public telephone is entitled 'to assume that the words he utters into the mouthpiece will not be broadcast to the world.'" *Smith*, 442 U.S. at 746 (Stewart, J., dissenting) (quoting *Katz*, 389 U.S. at 352).

If terms of service dictated expectations of privacy, private actors could unilaterally set the contours of Fourth Amendment protections. 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 form contracts.

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 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 747. Similarly, in *United States v. Owens*, this Court 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 at 150. And 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).

Even contract clauses that void an agreement based on criminality do not detract from the Fourth Amendment protections a user has against the government. In *United States v. Walton*, the defendant was driving a leased car on a suspended license and transporting large amounts of cocaine, despite the terms of the rental

agreement specifically voiding the contract if the car was used for illegal or other prohibited purposes. 763 F.3d 655, 656-57 (7th Cir. 2014). The Seventh Circuit held "the government's proposed standing exception—that drivers have no expectation of privacy in a rental car if they breach the rental agreement—would swallow the general rule" that renters have a legitimate expectation of privacy in rental cars over which they exert possession. *Id*. at 665.

C. Finding that Contractual Terms Impact a User's Expectation of Privacy Against the Government Would Lead to Absurd Results.

Finding terms of service and other agreements to be an indication of societal privacy understandings would lead to absurd results and would undermine well-established Fourth Amendment protections. In a case with similar facts, where the Southern District of New York held terms of use have no bearing on the defendant's reasonable expectation of privacy, that court noted:

> In today's world, meaningful participation in social and professional life requires using electronic devices—and the use of electronic devices almost always requires acquiescence to some manner of consent-to-search terms. If this acquiescence were enough to waive one's expectation of privacy, the result would either be (1) the chilling of social interaction or (2) the evisceration of the Fourth Amendment. Neither result is acceptable.

United States v. DiTomasso, 56 F. Supp. 3d 584, 592 (S.D.N.Y. 2014).[8] The lower

[8] Although *DiTomasso* held the defendant had a reasonable expectation of privacy in his email, the court also determined, without full analysis, that AOL acted as a

court's holding here would effectively mean email users would lose all privacy protections on the whim of whatever terms a provider may put in their user agreement, a result which would in turn chill private electronic communications.

The terms of service of 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] Broader still, Yahoo's TOS reserve the right to terminate users' accounts for "breaches or violations of the TOS or other incorporated agreements or guidelines," including such activities as sending content that is "racially, ethnically, or otherwise objectionable[;]" violates the "copyright or other proprietary rights . . . of any party[;]" or constitutes unsolicited

---

government agent when it scanned and shut down DiTomasso's email account. 56 F. Supp. 3d at 596. According to the court, in effectively agreeing to AOL's terms of service, DiTomasso consented to this "government" search. In contrast, this Court has determined that NCMEC, not AOL, acted as a government agent. *Ackerman*, 831 F.3d at 1295-1304.

[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/.

advertising.[11] And 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 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 your team at work without permission from the copyright holder, or marketing your small business to all of your friends without their advance consent. While some might find activities such as these 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.

The government's proposed rule in this case—that an email user's violation of a provider's terms of service extinguishes an expectation of privacy—raises more questions than it answers. Does it apply to the entirety of the account and all

[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.

[13] *Id.*

its contents, including years' worth of old emails? Does it apply to every terminated account, regardless of the reason for termination? Can the government conduct a baseless fishing expedition into the contents of an account after it is terminated? Does it mean that a subpoena for the *entirety* of every terminated user's account contents would not violate the Fourth Amendment? If this Court rejects the government's argument, it need not answer any of these questions.

III. A REASONABLE EXPECTATION OF PRIVACY DOES NOT END JUST BECAUSE AN ACCOUNT IS TERMINATED.

Even on its own terms, the district court's account termination rule does not hold up to scrutiny. Courts have recognized that an individual's expectation of privacy survives the termination of a contractual relationship in other analogous contexts. For example, in *Owens*, this Court held that a person maintains a reasonable expectation of privacy in the hotel room they continue to occupy, even after checkout time. 782 F.2d at 150. Similarly, both the Ninth and Eleventh Circuits have found that a lessee maintains a reasonable expectation of privacy in a rental car even after the rental agreement has expired. *See United States v. Henderson*, 241 F.3d 638, 647 (9th Cir. 2000); *United States v. Cooper*, 133 F.3d 1394, 1402 (11th Cir. 1998).

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

Likening email to a closed container, the Ninth Circuit 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, JK-15-029*, 828 F.3d 1083, 1091 (9th Cir. 2016). 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.

This could happen, however, if the unintended recipient decided to open the letter and report its contents to the government. Indeed, that is the premise of the "private search" doctrine as previously applied by this Court. *See Ackerman*, 831 F.3d at 1305-07 (citing *United States v. Jacobsen,* 466 U.S. 109 (1984); *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.)). Hence, as this Court explained, in *Jacobsen* the government's test of white powder from a package provided by

FedEx was not a search because it "'merely disclose[d]' whether the powder was contraband 'and no other arguably "private" fact.'" *Ackerman*, 831 F.3d at 1305-07 (quoting *Jacobsen*, 466 U.S. at 123). By contrast, in *Walter*, the FBI's "projection and viewing of films" labeled as obscene "*did* implicate the Constitution because the prior private search was much narrower, involving only the visual inspection of the labels on the outside of the film boxes." *Ackerman*, 831 F.3d at 1306 (citing *Walter*, 447 U.S. at 656-60)).

The line drawn in these private search cases 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 abrogated 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. *Lichtenberger*, 786 F.3d at 483-84. This Court

has already applied the private search doctrine to the facts here and found that NCMEC, as an agent of the government, exceeded the scope of AOL's prior inspection of the defendant's email. *Ackerman*, 831 F.3d at 1306-07. Had AOL's termination of the defendant's account defeated his expectation of privacy, the Court need not have engaged in this analysis at all.

IV. UPHOLDING THE DISTRICT COURT WOULD REINSTATE THE THIRD-PARTY DOCTRINE FOR EMAIL AND CREATE A SPLIT OF AUTHORITY WITH THE SIXTH CIRCUIT.

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. Finding a service provider could, through private contract terms, unilaterally abrogate this expectation of privacy would be a radical departure from the privacy people have long expected with respect to their personal communications. It would also create a split of authority with the Sixth Circuit.

Previously, this Court questioned whether *Smith v. Maryland* and its predecessor *United States v. Miller*, 425 U.S. 435 (1976), might apply here. It remanded for consideration of the application of the third-party doctrine to the defendant's email, specifically his "subjective expectations of privacy or the objective reasonableness of those expectations in light of the parties' dealings (*e.g.*, the extent to which AOL regularly accessed emails and the extent to which users

were aware of or acquiesced in such access)." *Ackerman*, 831 F.3d at 1305. But on remand, the government sought to frame the issue "narrowly," and in fact specifically disclaimed any reliance on the third-party doctrine. *Ackerman*, 2017 WL 4890433, at *3. Nevertheless, the district court answered that question by determining the defendant was aware of and agreed to AOL's TOS, which eliminated his expectation of privacy.

This is in direct conflict with *Warshak*, where 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 the possibility of 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. AOL's TOS here is not categorically different than the subscriber agreement in *Warshak*, which "contractually reserved the right to access Warshak's emails for certain purposes." *Id.* at 286. In particular, AOL's routine scanning of its subscribers' emails for "malware, viruses, and illegal images such as child pornography," *Ackerman*, 2017 WL 4890433, at *2, does not serve to place it beyond the reasonable expectation of privacy found by the Sixth Circuit. In its first consideration of *Warshak*, that court specifically addressed the government's

argument that email providers have tools to scan and sort email that would allow for the filtering of spam messages and the detection of child pornography. *Warshak v. United States*, 490 F.3d 455, 473-74 (6th Cir. 2007). The court held:

> [T]he fact that a computer scans millions of e-mails for signs of pornography or a virus does not invade an individual's content-based privacy interest in the e-mails and has little bearing on his expectation of privacy in the content.

Id. at 474.

Given this finding and the Sixth Circuit's ultimate holding the second time it addressed the issue in *Warshak*, 631 F.3d 266, upholding the district court here would create an unworkable split of authority. 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 Colorado, Kansas, New Mexico, Oklahoma, Utah, and Wyoming. 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*, 134 S. Ct. at 2491 (Fourth Amendment favors "clear guidance to law enforcement through categorical rules").

CONCLUSION

For the reasons above, the Court should reverse the district court and hold that Mr. Ackerman had a reasonable expectation of privacy in his email account, full stop, and the government violated that expectation when it accessed his email and its attached images without a warrant.

Dated: April 13, 2018

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 Amici Curiae Electronic Frontier Foundation, Brennan Center for Justice, and Center for Democracy and Technology

Barbara E. Bergman
Co-chair, NACDL Amicus Committee
James E. Rogers College of Law
The University of Arizona
1201 E. Speedway Drive
Tucson, AZ 85721
(505) 301-7547
bbergman@email.arizona.edu

Counsel for Amici Curiae National Association of Criminal Defense Lawyers

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 5,813 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: April 13, 2018

By: /s/ Jennifer Lynch
Jennifer Lynch

Counsel for Amici Curiae

CERTIFICATE OF DIGITAL SUBMISSION

I hereby certify that with respect to the foregoing:

(1) all required privacy redactions have been made per 10th Cir. R. 25.5;

(2) if required to file additional hard copies, that the ECF submission is an exact copy of those documents;

(3) the digital submissions have been scanned for viruses with the most recent version of a commercial virus-scanning program, Avast Mac Security Version 13.5, updated March 19, 2018, and according to the program are free of viruses.

Dated: April 13, 2018

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 13th day of April, 2018.

Dated: April 13, 2018

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