No. 18-30121

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

KALEB BASEY

Defendant-Appellant.

On Appeal from the United States District Court
for the District of Alaska, Fairbanks
No. 4:14-cr-00028-RRB-1
Hon. Ralph R. Beistline

BRIEF OF AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION & AMERICAN CIVIL LIBERTIES UNION OF ALASKA FOUNDATION IN SUPPORT OF DEFENDANT-APPELLANT KALEB BASEY

Brett Max Kaufman
Patrick Toomey
American Civil Liberties Union Foundation
125 Broad Street
New York, NY 10004
(212) 549-2500

Jennifer Stisa Granick
American Civil Liberties Union Foundation
39 Drumm Street
San Francisco, CA 94111
(415) 621-2493

Counsel for Amici Curiae

CORPORATE DISCLOSURE STATEMENT

Amici Curiae American Civil Liberties Union ("ACLU") and ACLU of Alaska Foundation are non-profit entities that do not have parent corporations. No publicly held corporation owns 10 percent of more of any stake or stock in amici curiae.

Date: February 19, 2019

/s/ Jennifer Stisa Granick
Jennifer Stisa Granick

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

STATEMENT OF INTEREST[1]

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

The ACLU of Alaska Foundation is an Alaska non-profit corporation dedicated to advancing civil liberties in Alaska; it is an affiliate of the American Civil Liberties Union. Like the national organization, the ACLU of Alaska Foundation has a long-time interest in protecting Alaskan's rights to privacy. The members and supporters of the ACLU of Alaska Foundation include individuals statewide who seek to ensure that they and their family members and friends receive fair and just treatment in the courts.[2]

---

[1] All parties consent to the filing of this brief. No party or party's counsel authored this brief or contributed money to fund the preparation or submission of this brief. No person other than amici, their members, and their counsel contributed money to fund the preparation or submission of this brief.

[2] Amici would like to thank Melodi Dincer and Kristin M. Mulvey, students in the Technology Law & Policy Clinic at NYU School of Law, for their contributions to this brief.

INTRODUCTION

Investigators in this case relied on 18 U.S.C. § 2703(f) to compel Yahoo! to copy and preserve Mr. Basey's emails and other account data—without getting a warrant—for nine months. This prolonged, warrantless seizure is typical of a growing nationwide practice: one where investigators regularly issue secret demands to preserve individuals' private account data just in case they decide to return with a court order later. Based on public transparency reports, federal and state investigators rely on section 2703(f) to copy and preserve private electronic data tens or hundreds of thousands of times each year. None of these demands require any showing of suspicion, need, or exigency.

The copying and preservation of Mr. Basey's emails and account data violated the Fourth Amendment. When Yahoo! secretly duplicated Mr. Basey's private data at the government's direction, it was acting as a government agent—and thus this seizure of his information was subject to Fourth Amendment constraints. In the absence of a warrant, copying and preserving these messages was an unconstitutional seizure of private information. A warrantless seizure can be justified by exigent circumstances if the government has good cause to preserve the data for a short while to seek a warrant. But if any exigency existed in this case—and none is apparent from the record—it dissipated over the nine months that the government delayed before applying for a warrant. Moreover, section

2703(f) is problematic because in most cases investigators appear to be using it to unconstitutionally seize private communications. The statute does not require probable cause, a risk that evidence will be destroyed, or that investigators promptly submit a court application to obtain the data they have preserved. While there may well be cases where the short-term, warrantless copying and preservation of private data is reasonable, this case is not one of them. The Court should hold that the government's protracted, warrantless seizure of Mr. Basey's private data violated the Fourth Amendment.

STATUTORY AND FACTUAL BACKGROUND

Every year, investigators use section 2703(f) to warrantlessly copy and preserve—for months at a time—the private data in tens or hundreds of thousands of internet accounts, including Mr. Basey's. This takes place because section 2703(f) gives law enforcement the power to unilaterally, and without suspicion or judicial approval, compel electronic communications service providers like Yahoo! to copy and preserve their users' email accounts.

The Stored Communications Act ("SCA") regulates government access to user data stored by electronic communications service providers (hereinafter "providers"), including Yahoo!. Under the SCA, some types of information, including certain account-related metadata, can be compelled from providers with a subpoena, while more sensitive data, including emails and other electronic

communications, require a court order or a search warrant. 18 U.S.C. § 2703. By contrast, section 2703(f) of the SCA establishes a procedure whereby investigators may themselves, without any judicial involvement, compel providers to make a copy of email messages and other account data, and preserve that copy for 90 days "pending the issuance of" legal process (or 180 days, with a renewal). The provider must comply.

Section 2703(f) reads:

> (1) In general.—
> A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.
>
> (2) Period of retention.—
> Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

Both the statutory text and the DOJ's own internal guidance documents indicate that the purpose of section 2703(f) is to give investigators the ability to ensure that relevant evidence will not be destroyed before law enforcement can obtain the requisite legal process compelling disclosure of private data.[3] The statute itself indicates that the government demand must be a precursor to seeking

[3] It is not clear that section 2703(f) permits law enforcement to seize the *content* of communications at all. The statute refers to "records and other evidence" and a "court order or other process." It does not specifically reference communications content nor the search warrants required to seize and search that information.

judicial authorization to obtain and search the data: requests must be made "pending the issuance of a court order or other process." 18 U.S.C. § 2703(f)(1). The Department of Justice ("DOJ") manual for Searching and Seizing Computers describes section 2703(f) as a means of preserving evidence so that it will not be "destroyed or lost before law enforcement can obtain the appropriate legal order compelling disclosure." DOJ, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 139 (2015), *available at* https://perma.cc/XYF8-J2KG. And the FBI's Domestic Investigations and Operations Guide instructs investigators that in order "to make a preservation request, the FBI must believe that the records will subsequently be sought by appropriate legal process." FBI, *Domestic Investigations and Operations Guide* 18-126 (2016), *available at* https://perma.cc/4DDY-942B.

However, the statute does not require Fourth Amendment safeguards. It does not require probable cause at the time law enforcement issues a copy and preservation demand. It does not require that there be a risk that evidence will be destroyed. Nor does it obligate investigators to seek legal process in a reasonable amount of time under the facts and circumstances of the case. Instead, it permits seizing information for up to 180 days without judicial oversight.

In practice, investigators issue tens or hundreds of thousands of boilerplate preservation demands under section 2703(f) each year—and often never return

with additional legal process. DOJ advises investigators to seek preservation "as soon as possible" after an investigation commences, and it provides a template for investigators to fill out. *See* DOJ, App. C Sample Language for Preservation Requests under 18 U.S.C. § 2703(f), *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 225–26 (2015), *available at* https://perma.cc/XYF8-J2KG. When investigators do return with a court order authorizing a search of the targeted account, they commonly wait months to do so. In theory, section 2703(f) appears intended to preserve records in cases where investigators have concrete intentions to seek legal process. But in practice, investigators regularly use the statute to force providers to copy and preserve tens or hundreds of thousands of private online accounts *just in case* a need for the information arises later in the course of an investigation.

Unsurprisingly, because section 2703(f) does not require probable cause or individualized suspicion and an independent judicial check—and because the government can issue demands under the statute quickly and simply—the volume of preservation demands is extremely high. Since at least July 2014, Google has annually received tens of thousands of 2703(f) letters requesting preservation of multiple user accounts—including 8,698 letters affecting 22,030 accounts in the

first half of 2018 alone.[4] Google, *Transparency Report: Requests for User Information (United States)*, https://perma.cc/MP98-8SCP (last visited Feb. 19, 2019). In that same six-month period, Facebook received 57,000 preservation letters for 96,000 different accounts. Facebook, *Transparency Report: Government Requests (United States)*, https://perma.cc/TVV5-QYW9 (last visited Feb. 19, 2019) ("Facebook Transparency Report"). In recent years, these numbers have been rising. Comparing to the six-month period between July and December 2017 with the period between January and June 2018, Google and Facebook together experienced between 20% and 30% increases in section 2703(f) letters and affected accounts.

In some of these instances, investigators eventually meet the constitutional and statutory standards required to search private account data by subsequently serving appropriate legal process on providers. But providers receive thousands more section 2703(f) letters than they do subsequent legal process to actually search the accounts. For example, in the most recent six-month reporting period, Facebook received a total of 57,000 section 2703(f) letters, but only received 23,801 search warrants, 9,369 subpoenas, and 942 section 2703(d) court orders.

[4] One letter can require a provider to copy and retain emails and other data from more than one account.

Id.[5] Even assuming—implausibly—that legal process is always tied to an account previously targeted by a section 2703(f) letter, investigators never demonstrated any basis for their demands to copy and preserve accounts on almost 23,000 occasions over six months. From this data, it appears that the government's actual use of section 2703(f) is not primarily about preservation of evidence in cases where investigators are actively seeking a warrant. Rather, section 2703(f) provides investigators with a powerful tool to routinely copy and preserve tens of thousands of accounts without any evidence, risk of spoliation, judicial oversight, or obligation to follow-up.

Making matters worse, investigators appear to rarely formally renew section 2703(f) demands (or seek related judicial process) within the statutorily provided 90-day retention period—or even within 180 days, after the one renewal contemplated by the statute. Indeed, one district court recently noted that the case at issue was "the first time the Court can remember the government indicating it renewed its preservation request" within the allotted 90 days. *In the Matter of the Search of premises known as: Three Hotmail Email accounts*, No. 16-MJ-8036-DJW, 2016 WL 1239916, at * 12 n.78 (D. Kan., Mar. 28, 2016), *overruled in part on other grounds*, 212 F. Supp. 3d 1023 (D. Kan. 2016). According to the court, it

[5] Section 2703(d) allows the government to obtain certain account data upon a showing of "specific and articulable facts showing that there are reasonable grounds to believe that [the data sought] are relevant and material to an ongoing criminal investigation."

was also "the first time the Court can remember the government *seeking* a search warrant within that one-time renewal period, as seems to be the intent of subsection (f)." *Id.* There, the records were preserved beyond the 180-day statutory maximum and it appears the government never requested an extension of time.[6]

As both data and anecdote demonstrate, law enforcement officers regularly send section 2703(f) requests as a "matter of course," copying and preserving troves of personal data for months at a time, without any showing of cause or need. Orin Kerr, *The Fourth Amendment and Email Preservation Letters*, Wash. Post: The Volokh Conspiracy, Oct. 28, 2016, https://wapo.st/2IdmLjv ("[T]he preservation authority is routinely used by the government to preserve contents of communications. . . . And it turns out that a lot of investigators and prosecutors issue such letters often."). As explained above, this offends the statute—and, as discussed below—the Fourth Amendment as well.

ARGUMENT

I. The Government's Use of Section 2703(f) in Mr. Basey's Case Violated the Fourth Amendment.

The government's use of section 2703(f) to copy and preserve Mr. Basey's email account data violated the Fourth Amendment. Although warrantless seizures of email accounts may be justified in certain cases involving exigent circumstances, this case is not one of them. Congress could write a statute that

[6] As discussed below, the same sequence of events occurred in this case.

lawfully requires providers to temporarily retain data at risk of spoliation for a short period of time while law enforcement seeks a warrant. But section 2703(f) authorizes law enforcement to seize emails—private property—far beyond what the Fourth Amendment allows. Without probable cause, or case-specific reasons to believe that evidence will be destroyed, the statute forces communications providers to copy and preserve communications for months at a time. These seizures are unconstitutional.

A. The Government Compelled Yahoo! to Copy and Preserve Mr. Basey's Private Data for Nine Months Without a Warrant.

The government's use of section 2703(f) in this case exemplifies how investigators regularly rely on this provision to carry out protracted, warrantless seizures of personal communications.

In this case, three law enforcement agencies were investigating Mr. Basey for attempted enticement of a minor in violation of 18 U.S.C. § 2422(b), receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2) and (b)(1), and distribution of child pornography in violation of 18 U.S.C. § 2252(a)(2) and (b)(1). Indictment, *United States v. Basey*, No. 4:14-cr-00028-RRB (D. Alaska Dec. 16, 2014). These agencies included the Alaska State Troopers ("AST"), the United States Army Criminal Investigation Command ("CID"), and the Federal Bureau of Investigation ("FBI"). Br. for Appellant at 2–3, *United States v. Basey*, No. 18-3012 (9th Cir. Feb. 12, 2019), ECF No. 26. As part of the investigation, in January

of 2014, officials seized Basey's electronic devices. *Id.* at 6. Almost one month later, on February 7, 2014, CID agent Shanahan sent a section 2703(f) letter to Yahoo!, requiring the company to preserve Basey's email account for 90 days. *Id.* at 6. Four days later, on February 11, Yahoo! confirmed with investigators that it had preserved Basey's account. *Id.* at 6–7. From May to June of 2014, AST searched Basey's devices (but not his Yahoo! account) pursuant to a military search warrant. *Id.* Based on information obtained through this search, AST and CID then contacted the FBI, which used a subpoena to obtain Craigslist[7] postings sent from Basey's Yahoo! email address. *Id.* Finally, on November 11, 2014—more than nine months after issuing a section 2703(f) demand to Yahoo!—the FBI secured a warrant for the Yahoo! account. The FBI then obtained the data preserved under section 2703(f) and searched Basey's Yahoo! emails, producing the evidence used to convict him in this case.

This use of section 2703(f) is typical in that investigators do not appear to have issued the demand when they were actively seeking a warrant to take possession of and search Mr. Basey's Yahoo! data—nor did they obtain legal process within the statutorily prescribed time period. These failures both afflicted this investigation, and also fit a pattern that appears common in criminal

[7] Craigslist is a popular online forum hosting classified advertisements for jobs, housing, items wanted and for sale, as well as discussion forums.

investigations that involve potential searches of digital data—which, in today's world, is practically all investigations.

B. The Fourth Amendment Protects the Content of Email Communications Against Warrantless Searches and Seizures.

The Fourth Amendment provides that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV. The Fourth Amendment protects both an individual's reasonable expectation of privacy and her property rights. This constitutional protection means that the government generally must obtain a warrant before searching or seizing private property. *Katz v. United States*, 389 U.S. 347, 357 (1967).

Email and other electronic communications are among those personal effects protected by the Fourth Amendment. Email can contain the most private and personal messages imaginable. *See, e.g.*, *Riley v. California*, 134 S. Ct. 2473, 2490, 2494–95 (2014). Today we use email and text messages 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." *United States v. Warshak*, 631 F.3d 266, 284 (6th Cir. 2010). 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); *see Warshak*, 631 F.3d at 284 ("Since the advent of email, the telephone call and the letter have waned in importance, and an explosion of Internet-based communications has taken place."); *see also Kyllo v. United States*, 533 U.S. 27, 28 (2001) (cautioning that advances in technology must not "erode the privacy guaranteed by the Fourth Amendment").

Because of its sensitivity, the Fourth Amendment protects email and other similar modes of communication from unreasonable searches and seizures. *See Katz*, 389 U.S. at 353; *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[.]"); *In re Grand Jury Subpoena*, 828 F.3d 1083, 1090 (9th Cir. 2016) ("Personal email can, and often does, contain all the information once found in the 'papers and effects' mentioned explicitly in the Fourth Amendment."); *United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2008) (holding that "[t]he privacy interests in [mail and email] are identical"); *Warshak*, 631 F.3d at 284, 288 (holding that an individual enjoys a reasonable expectation of privacy in the contents of emails); *cf. Ex parte Jackson*, 96 U.S. 727, 733 (1877) (Fourth Amendment protects letters in transit). Indeed, in the Supreme Court's recent opinion in *United States v. Carpenter*, every Justice

agreed, at least in dicta, that the Fourth Amendment protects the content of emails. *See* 138 S. Ct. 2206, 2222 (2018) (majority op.); *id.* at 2230 (Kennedy, J., dissenting, joined by Thomas and Alito, JJ.); *id.* at 2262, 2269 (Gorsuch, J., dissenting).[8]

Widespread adoption of email and other electronic communications has led to a societal recognition that these materials are extremely private. That recognition goes hand in hand with the longstanding possessory interest people have in their email messages, as well as the growing number of statutes that seek to manage property rights in intangible data.

Like the privacy interest, the Fourth Amendment also protects the property interest in email. The Fourth Amendment protects an individual's possessory interest in her papers and effects. *See Soldal v. Cook Cty.*, 506 U.S. 56, 62–64, 68 (1992) (explaining that a seizure occurs when one's property rights are violated, even if the property is never searched). Possessory interest is defined as the present "right to control property, *including the right to exclude others*, [even] by a person who is not necessarily the owner." Black's Law Dictionary (10th ed. 2014) (emphasis added); *United States v. 1982 Sanger 24' Spectra Boat*, 738 F.2d 1043,

[8] Besides communications content, an email subscriber may have a reasonable expectation of privacy in other categories of account information, such as certain account metadata. Since the government seized the content of Basey's communications, this Court need not decide here whether the Fourth Amendment also protects the other types of data that the government seized when it directed Yahoo! to preserve Basey's account.

1046 (9th Cir. 1984); *Loretto v. Teleprompter Manhattan CA TV Corp.*, 458 U.S. 419, 435 (1982) ("The power to exclude has traditionally been considered one of the most treasured strands in an owner's bundle of property rights."). A possessory interest also includes the right to delete or destroy the property. *United States v. General Motors Corp.*, 323 U.S. 373, 378 (1945) (Property rights in a physical thing have been described as the rights "to possess, use and dispose of it." (quotation marks omitted)); *cf. United States v. Carpenter*, 484 U.S. 19, 26 (1987) ("Confidential business information has long been recognized as property.").

Email has these canonical characteristics of property. Users have the right to exclude others from their accounts. Users protect their accounts with passwords. Providers encrypt user emails both in transit and when stored on servers in order to exclude outsiders. Email users also have the right to delete their email messages. Providers allow users to delete single messages, or the entire account. And even though email is intangible, it is still property subject to Fourth Amendment protections. *Hoffa v. United States*, 385 U.S. 293, 301 (1966) (Fourth Amendment protections are "surely not limited to tangibles . . . ."); U*nited States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir.1986) ("[S]urreptitious searches and seizures of intangibles strike at the very heart of the interests protected by the Fourth Amendment."); *Katz*, 389 U.S. at 353; *Berger v. New York*, 388 U.S. 41, 54–60 (1967) (telephone conversations); *United States v. Biasucci*, 786 F.2d 504, 509–10

(2d Cir. 1986) (video surveillance); *United States v. Torres*, 751 F.2d 875, 883 (7th Cir. 1984) (video surveillance); *United States v. Taborda*, 635 F.2d 131, 139 (2d Cir. 1980) (enhanced visual surveillance inside the home). Moreover, the Fourth Amendment protects emails even if a provider's terms of service or privacy policy allow government access under certain circumstances, as almost all do. Courts have considered and rejected arguments to the contrary. *See, e.g.*, *Warshak*, 631 F.3d at 286 ("While . . . a subscriber agreement might, in some cases, be sweeping enough to defeat a reasonable expectation of privacy in the contents of an email account . . . we doubt that will be the case in most situations . . . ."); *United States v. Heckenkamp*, 482 F.3d 1142, 1146-47 (9th Cir. 2007) (policies establishing limited instances of access do not vitiate Fourth Amendment interests).

State laws recognize that individuals are the owners of the data in their email accounts. State legislatures are increasingly recognizing a property right in electronic communications. For example, the Texas Property Code defines "[p]roperty" for the purposes of trust management as "including property held in any digital or electronic medium." Tex. Prop. Code Ann. § 111.004(12) (2017). Missouri amended its state constitution in 2014 to protect "persons, papers, homes, effects, *and electronic communications and data*, from unreasonable searches and seizures[.]" Mo. Const. art. I, § 15 (emphasis added); *see also* Becca Stanek, *Missouri Passes Constitutional Amendment to Protect Electronic Privacy*, Time

Magazine, Aug. 6, 2014, https://perma.cc/56D3-RUUR. Similarly, California's Electronic Communications Privacy Act prohibits government entities from compelling production of or access to electronic communications without a warrant. Cal. Penal Code § 1546.1 (2016).

In some states, legislatures have made clear that email account information is property in the context of determining rights after incapacity or death. Over the past several years, a wave of state legislatures enacted laws addressing access to "digital assets," including email accounts, upon a person's incapacity or death. *See generally Access to Digital Assets of Decedents*, Nat'l Conf. of State Legs. (Dec. 3, 2018), https://perma.cc/Z35T-AS45; Natalie M. Banta, *Inherit The Cloud: The Role of Private Contracts in Distributing or Deleting Digital Assets At Death*, 83 Fordham L. Rev. 799, 801 (2014) (defining "digital assets" to "include an individual's email accounts"). These laws extend fiduciary duties to electronic communications as another form of property that can be held in trust. For example, Alaska's Fiduciary Access to Digital Assets Act conditions disclosure of the electronic communications of a deceased user upon their prior consent or on a court order. Alaska Stat. Ann. § 13.63.040 (2017). Since 2013, at least 46 states have enacted similar laws regulating fiduciary duties with respect to digital assets, all of which explicitly recognize a deceased or incapacitated user's legal interest in

access to their email communications.[9] Wisconsin's version is of particular note, as the statutory chapter is entitled "Digital Property." Wisc. Stat. Ann. § 711 (2016).

Additionally, some state courts have also begun to expand common law property principles to better protect digital communications. *See, e.g.*, *Ajemian v. Yahoo!, Inc.*, 478 Mass. 169, 170 (2017) (finding e-mail accounts are a "form of property often referred to as a 'digital asset'"); *Eysoldt v. ProScanImaging*, 194 Ohio App. 3d 630, 638 (2011) (permitting conversion action of web account as intangible property).

Because email is private personal property, it is protected by the Fourth Amendment from unreasonable searches and seizures.

C. Yahoo! Acted as a Government Agent When It Copied and Preserved Mr. Basey's Email Account Pursuant to Section 2703(f).

Although the Fourth Amendment does not apply to private entities, Yahoo! acted as a government agent here when it copied and preserved Basey's email at

[9] *See*, *e.g.*, Ariz. Rev. Stat. Ann. §§ 14-13101 to -13118 (2016); Cal. Prob. Code §§ 870–84 (2017); Colo. Rev. Stat. Ann. §§ 15-1-1501 to -1518 (2016); Conn. Gen. Stat. Ann. §§ 45a-334b-339 (2016); Del. Code Ann. tit. 12, §§ 5001-5007 (2015); Fla. Stat. §§ 740.001-.09 (2016); Hawaii Rev. Stat. §§ 556a-1 to -17 (2016); Idaho Code §§ 15-14-101 to -119 (2016); 755 Ill. Comp. Stat. 70/1 to -21 (2016); Ind. Code §§ 32-39-1-1 to -2-15 (2016); Md. Code Ann. Est. & Trusts §§ 15-601 to -620 (2016); Mich. Comp. Laws §§ 700.1001-.1018 (2016); Minn. Stat. §§ 521a.01-.19 (2016); Neb. Rev. Stat. §§ 30-501 to 508 (2016); N.Y. Est. Powers & Trusts Law §§ 13-a-1 to -5.2 (2016); N.C. Gen. Stat. Ann. §§ 3f-1 to -18 (2016); S.C. Code Ann. §§ 62-2-1010 to -1090 (2016); Tenn. Code Ann. §§ 35-8-101 to 118 (2016); Wash. Rev. Code Ann. §§ 11.120.010-.901 (2016); Wisc. Stat. § 711.01 (2016).

the government's behest. Yahoo!'s actions, then, must comply with the Fourth Amendment.

Private entities are state actors when the government directs their activities. In *United States v. Miller*, this Court created a two-prong test to discern whether a private individual is acting as a governmental agent or instrument for Fourth Amendment Purposes: "(1) whether the government knew of and acquiesced in the intrusive conduct, and (2) whether the party performing the search intended to assist law enforcement efforts or to further [their] own ends." 688 F.2d 652, 657 (9th Cir. 1982); *see United States v. Reed*, 15 F.3d 928, 931 (9th Cir. 1994).

When companies comply with section 2703(f) letters, they are acting as agents of the government—just as they are when they actually retrieve and produce customer data in response to court-approved legal process. Here, Yahoo!, a private company, acted as a governmental agent because (1) the investigating agencies involved in Mr. Basey's case not only knew of but directed the search and seizure, and (2) Yahoo! preserved Mr. Basey's entire email account for the purpose of complying with investigators' section 2703(f) demand, not for its own purposes. *See In the Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, 829 F.3d 197, 214 (2d Cir. 2016) (holding, in another case involving the Stored Communications Act, that "[w]hen the government compels a private party to assist it in conducting a search or seizure,

the private party becomes an agent of the government" under the Fourth Amendment), *vacated as moot by United States v. Microsoft*, 138 S. Ct. 1186 (2018).

D. The Copying and Preservation of Mr. Basey's Emails Was a Seizure Under the Fourth Amendment.

When the government sent Yahoo! a section 2703(f) demand requiring copying and preservation of Basey's email and other messages, it was a Fourth Amendment seizure. A Fourth Amendment "seizure" of property occurs when "there is some meaningful interference with an individual's possessory interests in that property." *Jacobsen*, 466 U.S. at 113; *Horton v. California*, 496 U.S. 128, 133 (1990). Yahoo!'s compliance meant that Basey could no longer exclude the government from accessing, searching, using, or sharing his private messages and associated data. It meant that he could no longer delete his messages. Because of the receipt of the 2703(f) letter, whatever the user did to his information, a copy would nevertheless remain for government use. That copying and preservation meaningfully interfered with his possessory interests—and thus constituted a Fourth Amendment seizure.

The government may argue that it neither took possession of nor reviewed Basey's emails prior to obtaining a warrant. This is irrelevant. The warrantless seizure took place at the point in time when the government's agent, Yahoo!, copied the account data. Human examination is not required for a seizure. Rather, a

seizure occurs when police secure or detain private property so that they may search it later. The Supreme Court has flatly rejected the view that the Fourth Amendment only protects property seizures where there is a corresponding privacy or liberty invasion. *See Soldal*, 506 U.S. at 62–65 (holding that dragging away a mobile home was a seizure even though officers had not entered the house, rummaged through the possessions, or detained the owner). Similarly, in *United States v. Place*, the seized a container and did not allow anyone to touch it or its contents while the police obtained a search warrant—but the Court held this was a seizure governed by the Fourth Amendment. 462 U.S. 696, 707 (1983) ("There is no doubt that the agents made a 'seizure' of Place's luggage for purposes of the Fourth Amendment when, following his refusal to consent to a search, the agent told Place that he was going to take the luggage to a federal judge to secure issuance of a warrant."). Likewise, private account data is seized at the moment that providers copy and preserve that information pursuant to the government's demand. The section 2703(f) letter process interferes with an email account holder's Fourth Amendment-protected interests even if an investigator never examines the materials.

E. The Government's Warrantless Seizure of Mr. Basey's Private Information Was Unreasonable.

The government seized Basey's emails without a warrant when Yahoo! copied the data for investigators. The record here does not justify this warrantless

seizure, especially not for nine months. The seizure of Basey's emails was unreasonable and unconstitutional.

It is a cardinal Fourth Amendment rule that "[a] seizure conducted without a warrant is per se unreasonable . . . subject only to a few specifically established and well-delineated exceptions." *Sandoval v. Cty. of Sonoma*, 912 F.3d 509, 515 (9th Cir. 2018); *United States v. Hawkins*, 249 F.3d 867, 872 (9th Cir. 2001) (quoting *Minnesota v. Dickerson*, 508 U.S. 366, 372 (1993)). "When the right of privacy must reasonably yield to the right of search (and seizure) is, as a rule, to be decided by a judicial officer, not by a policeman or Government enforcement agent." *United States v. McCormick*, 502 F.2d 281, 285 (9th Cir. 1974) (quoting *Johnson v. United States*, 333 U.S. 10, 14 (1948)). Review by a neutral and objective judicial magistrate who weighs the importance of the constitutional safeguards of the Fourth Amendment with law enforcement interests helps ensure law enforcement actions are not abusive or unjustified. The purpose of requiring a warrant is to minimize the risk of "arbitrary invasions by governmental officials" to the "privacy and security of individuals[.]" *Camara v. Municipal Ct.*, 387 U.S. 523, 528 (1967). The warrant process "'assures the individual whose property is searched or seized of the lawful authority of the executing officer, his need to search, and the limits of his power to search.'" *Groh v. Ramirez*, 540 U.S. 551, 561 (2004) (quoting *United States v. Chadwick*, 433 U.S. 1, 9 (1977)). In other words,

the warrant specifically describing the items to be seized legitimates an officer's authority to seize those items. *See San Jose Charter of the Hells Angels Motorcycle Club v. City of San Jose*, 402 F.3d 962, 973 (9th Cir. 2005).

Here, no warrant authorized the government's seizure of Mr. Basey's email account. Thus, the government bears the burden of showing that its warrantless seizure falls "under one of a few specifically established exceptions to the warrant requirement." *United States v. Huguez-Ibarra*, 954 F.2d 546, 551 (9th Cir. 1992). No exception applies.

The government may argue that Basey consented to the seizure of his account via the Yahoo! terms of service or privacy policy. But these materials do not vitiate users' Fourth Amendment interests. Courts have repeatedly rejected the argument that they do. *See e.g.*, *Warshak*, 631 F.3d at 286; *Heckenkamp*, 482 F.3d at 1146-47; *Carpenter*, 138 S. Ct. at 2220; *see also supra* Section I.B. Nearly every terms of service and privacy policy states that the provider may disclose information pursuant to valid legal process and legal requests. That is a statement of fact, not an expression of consent. If these notices authorized warrantless seizures and searches, most of our email communications would lack Fourth Amendment protection. As the courts have repeatedly made clear, that is hardly the case.

More to the point, the government may argue that this warrantless seizure was justified to preserve evidence pending investigators' application for a search warrant. Under the exigency exception to the warrant requirement, a warrantless search or seizure may nevertheless be constitutional if: "(1) [officers] have probable cause to believe that the item or place . . . contains evidence of a crime, and (2) they are facing exigent circumstances that require immediate police action." *United States v. Camou*, 773 F.3d 932, 940 (9th Cir. 2014); *see United States v. Ojeda*, 276 F.3d 486, 488 (9th Cir. 2002). The circumstances must "cause a reasonable person to believe that entry or search was necessary to prevent physical harm . . . the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts." *Camou*, 773 F.3d at 940 (alterations and citations omitted). Thus, the exigency exception applies when officers are in "hot pursuit" of a fleeing suspect, the suspect might threaten the safety of police or others, or when evidence of the crime or contraband might be destroyed. *See Warden v. Hayden*, 387 U.S. 294 (1967) (fleeing suspect); *Ryburn v. Huff*, 565 U.S. 469 (2012) (threat of injury); *Kentucky v. King*, 563 U.S. 452, 455 (2011) (destruction of contraband).

The government has not met its burden to establish exigency here. The record does not appear to establish probable cause to seize or search Basey's email account at the time investigators sent the section 2703(f) letter to Yahoo!. Email

accounts contain highly sensitive information and the invasion of privacy and interference with property is extreme. Without probable cause, the government has no demonstrable right to the information, and its seizure is unreasonable. *See Camou*, 773 F.3d at 940.

The need to preserve evidence that might be destroyed can justify a warrantless seizure, but only for as long as the exigency lasts. The exigency exception is limited to the length of the exigency itself. *See Mincey v. Arizona*, 437 U.S. 385 (1978). A warrantless search or seizure under the exigency exception must be limited in scope so that it is "strictly circumscribed by the exigencies which justify its initiation." *Id*. at 393. At some point, the duration of a seizure can exceed the time required to promptly prepare and obtain a warrant—rendering the seizure unreasonable.

If investigators reasonably believed that the contents of Mr. Basey's account could be destroyed, it is beyond imagination that exigency lasted for nine months—beyond even what the statute permits. Even if initially copying Basey's emails was lawful, retaining them for nine months was not. The Fourth Amendment governs both the initial copying of data and also its retention. Given how strong the individual's privacy and property interests are, and the weak government interest in stockpiling private communications in the absence of any genuine exigency, this ongoing retention was unreasonable as well. In *Mincey*, the

Supreme Court held that a four-day long warrantless search of appellant's apartment following a shoot-out was impermissible, even though the investigators were initially legitimately at the premises and investigating a murder. *Mincey*, 437 U.S. at 394. In *Place*, the Court suppressed evidence obtained after investigators detained the defendant's luggage for ninety minutes. *Place*, 462 U.S. at 696, 710. The Court held that "the length of the detention of respondent's luggage *alone* precludes the conclusion that the seizure was reasonable in the absence of probable cause." *Id.* at 709 (emphasis added).

Thus, in both *Mincey* and *Place*, an initial seizure was justified by exigency. But prolonged interferences with Fourth Amendment interests converted lawful police action into unconstitutional ones. Likewise, here, because the government compelled the retention of Basey's data long past any time period necessary to obtain legal process, that seizure was unreasonable.

F. Section 2703(f) Forces Providers to Perform Unconstitutional Seizures on Behalf of Law Enforcement.

The statute authorizes warrantless seizures that last 90 days by default and are untethered from any showing of exigency. The Fourth Amendment requires more than that to justify such a warrantless intrusion. Section 2703(f) states that a provider must preserve records "pending the issuance of a court order or other process." But the statute does not contain any judicial oversight, notice, or obligation to seek a warrant within a reasonable amount of time. 18 U.S.C.

§ 2703(f). As a result, investigators routinely copy and preserve private email account information just in case. Sometimes the police come back for the data months later. Sometimes they do not. *See supra* Statutory and Factual Background. Meanwhile, the most sensitive of our personal materials is preserved in anticipation of government perusal at some undetermined future point.

The need to preserve evidence is a legitimate law enforcement interest. But officers must have probable cause to believe that the item contains evidence of a crime, and must be facing exigent circumstances that require immediate police action. *Camou*, 773 F.3d 932, 940. Section 2703(f) also does not limit the seizures it authorizes to the *length* of the exigency as the Fourth Amendment requires. *Mincey*, 437 U.S. 385. Instead, section 2703(f) provides a 90- or 180-day retention period, regardless of the facts of the case. It is hard to imagine any situation where the government has the requisite probable cause but needs 90 days or more to seek a warrant.

Congress could pass a statute that would lawfully obligate providers to preserve account information in exigent circumstances. At the very least, a constitutional statute would authorize law enforcement to make preservation demands if investigators have probable cause, are in the process of seeking a warrant, and there is a risk of spoliation. In that situation, upon receipt of the demand, a provider could be required copy and retain the data for a short period of

time while the government applies for the warrant. Unfortunately, to the detriment of tens or even hundreds of thousands of people each year, this is not what section 2703(f) does.

CONCLUSION

Mr. Basey's emails were warrantlessly seized for nine months, an unreasonable amount of time for law enforcement to interfere with an individual's powerful constitutional interest in these private and personal digital papers. For these reasons, this Court should hold that the government's seizure of Mr. Basey's Yahoo! emails pursuant to section 2703(f) violated the Fourth Amendment.

Date: February 19, 2019

Respectfully submitted,

/s/ Jennifer Stisa Granick
American Civil Liberties Union Foundation
Jennifer Stisa Granick
39 Drumm Street
San Francisco, CA 94111-4805

Brett Max Kaufman
Patrick Toomey
American Civil Liberties Union Foundation
125 Broad Street
New York, NY 10004
(212) 549-2500

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify that:

This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 6,553 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionately spaced typeface using Times New Roman 14-point font.

Date: February 19, 2019

/s/ Jennifer Stisa Granick
Jennifer Stisa Granick

CERTIFICATE OF SERVICE

I hereby certify that on February 19, 2019, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system.

Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

Date: February 19, 2019

/s/ Jennifer Stisa Granick
Jennifer Stisa Granick