No. _____

In The
Supreme Court of the United States

KALEB LEE BASEY,
Petitioner,

v.

UNITED STATES OF AMERICA,
Respondent.

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

PETITIONER'S APPENDIX

Kaleb Lee Basey
17753-006 Cardinal Unit
Federal Medical Center Lexington
P.O. Box 14500
Lexington, KY 40512-4500
Petitioner in Pro Se

TABLE OF CONTENTS

APPENDIX **Page**

NOT FOR PUBLICATION

FILED

AUG 14 2019

MOLLY C. DWYER, CLERK
U.S. COURT OF APPEALS

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. KALEB L. BASEY, Defendant-Appellant.	No. 18-30121 D.C. No. 4:14-cr-00028-RRB MEMORANDUM*

Appeal from the United States District Court
for the District of Alaska
Ralph R. Beistline, District Judge, Presiding

Argued and Submitted August 5, 2019
Anchorage, Alaska

Before: TALLMAN, IKUTA, and N.R. SMITH, Circuit Judges.

Kaleb Basey was convicted by a jury of one count of transportation of child pornography and one count of distribution of child pornography, in violation of 18 U.S.C. § 2252(a)(1), (a)(2), and (b)(1). Basey appeals the district court's denials of his request for a continuance in order to file additional suppression motions, his motion to dismiss the indictment on speedy trial grounds, and his motion for

* This disposition is not appropriate for publication and is not precedent except as provided by Ninth Circuit Rule 36-3.

judgment of acquittal under Federal Rule of Criminal Procedure 29. We have jurisdiction under 28 U.S.C. § 1291, and we affirm.

1. We review the denial of a motion to continue for abuse of discretion. *See United States v. Soto*, 794 F.3d 635, 655 (9th Cir. 2015). It is undisputed that Basey made his request for a continuance to file additional suppression motions: (a) twelve days before trial was set to begin; (b) eight months after the last stated pretrial motions deadline; and (c) following two complete rounds of pretrial suppression motions he had previously filed. Basey's renewed request was untimely under Federal Rule of Criminal Procedure 12(c)(3), and he was required to show good cause why the district court nevertheless should consider it. *See United States v. Tekle*, 329 F.3d 1108, 1112 (9th Cir. 2003) (addressing then-current Rule 12(f)). Based on this record, we cannot say that the district court abused its discretion when it denied Basey's motion to continue.[1]

2. We review the district court's denial of a Sixth Amendment speedy trial

[1] We reject Basey's argument that the district court must have reached the merits of his proposed motions in denying the continuance because it stated that the motions "all appear to be without merit on their face." Because the court made no findings (explicit or implicit) respecting whether Basey's email account was seized under 18 U.S.C. § 2703(f) in violation of the Fourth Amendment, let alone whether his emails should be suppressed, *cf. United States v. Scott*, 705 F.3d 410, 416 (9th Cir. 2012) (to constitute a ruling on the merits of a waived or forfeited suppression argument, a court's order must actually determine whether seized evidence should have been suppressed), we are not persuaded that the merits, and not the untimely nature of the motion, was the basis of the court's ruling.

claim de novo, reviewing the underlying findings of fact for clear error. *See United States v. Sutcliffe*, 505 F.3d 944, 956 (9th Cir. 2007). To determine whether Basey's Sixth Amendment rights were violated, we must balance "the length of the delay, the reason for the delay, the defendant's assertion of his right, and prejudice to the defendant." *United States v. Tanh Huu Lam*, 251 F.3d 852, 855 (9th Cir. 2001) (citing *Barker v. Wingo*, 407 U.S. 514, 529 (1972)). Though the delay in this case was long enough to trigger the *Barker* balancing test, we conclude that the balance of factors here ultimately does not weigh in Basey's favor.

The second *Barker* factor—the reason for the delay—is the "focal inquiry" in the analysis. *See United States v. King*, 483 F.3d 969, 976 (9th Cir. 2007). The district court's finding that Basey was largely responsible for the delay is not clearly erroneous. The record supports the court's conclusion that most, if not all, of the delay was due to the sequential manner in which Basey chose to file his pretrial motions and his decision to change counsel less than a month before his trial date. As to the third factor, Basey did not assert his right to a speedy trial until after all of his other pretrial motions had been resolved and he was approaching the eve of trial. This does not "strongly counsel in favor of finding a Sixth Amendment violation." *Id.* Finally, while Basey's pretrial confinement—whether measured from the date of the superseding indictment or the first indictment—was

lengthy, it still must be "balanced and assessed in light of the other *Barker* factors, including the . . . reasons[] and responsibility for the delay." *Lam*, 251 F.3d at 860. Under the circumstances of this case, we conclude that Basey's Sixth Amendment right to a speedy trial was not violated since he was primarily responsible for delays.

3. We review de novo the denial of a Rule 29 motion for acquittal and examine the sufficiency of the evidence to convict. *See United States v. Tisor*, 96 F.3d 370, 379 (9th Cir. 1996). Here, the evidence at trial, taken in the light most favorable to the prosecution, was sufficient for a rational juror to find the essential elements of Basey's crimes beyond a reasonable doubt and the venue properly laid in the District of Alaska.[2] *See United States v. Doe*, 842 F.3d 1117, 1119 (9th Cir. 2016). Even assuming that the child pornography distribution charge at issue here required proof that a recipient opened the email attachment of a pornographic image, the jury reasonably could have concluded from the emails produced at trial that the recipient of Basey's email did so. Likewise, as to his claim that venue was not proper in Alaska, a rational fact finder could conclude that it was more likely than not that Basey emailed a child pornography image to himself on October 22, 2013, while he was in Fairbanks, Alaska, and that venue there was proper.

[2] Venue need only be shown by a preponderance of the evidence. *See United States v. Lukashov*, 694 F.3d 1107, 1120 (9th Cir. 2012).

AFFIRMED.

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, Plaintiff, vs. KALEB LEE BASEY, Defendant.	Case No. 4:14-cr-00028-RRB-SAO **ORDER DENYING MOTION TO CONTINUE TRIAL**

Before the Court at Docket 166 is Defendant's seventh Motion to Continue Trail. The Government opposed at Docket 169 and the Court held a hearing in the matter on June 30, 2017. Thereafter each of the parties briefed the issue.

Defendant seeks a seventh continuance in order to file additional motions to suppress, contending that there are new issues of substance that must be resolved prior to trial. The Government disputes these assertions, and the Court has independently studied the matter. As the Government points out at Docket 172, most, if not all, of the issues that Defendant seeks to address by motion practice already have been addressed and resolved by the Court, and all appear to be without merit on their face.

Therefore, for the reasons set forth by the Government at Docket 172, the Motion to Continue Trial is hereby DENIED. Defendant has had ample time and opportunity to file pretrial motions and now appears to be motivated primarily for delay.

Appendix B

There is a status hearing set for Thursday July20, 2017, in Fairbanks, Alaska. At that time, the parties shall notify the Court when they will be ready for trial.

IT IS SO ORDERED this 18th day of July, 2018, at Anchorage, Alaska.

/s/ Ralph R. Beistline
RALPH R. BEISTLINE
Senior United States District Judge

UNITED STATES DISTRICT COURT

District of Alaska

UNITED STATES OF AMERICA
v.
KALEB L. BASEY

JUDGMENT IN A CRIMINAL CASE
(For **Supervised Release**)

Case Number: 4:14-CR-00028-01-RRB

USM Number: 17753-006

Rex Lamont Butler
Defendant's Attorney

THE DEFENDANT:

☐ pleaded guilty to count(s) _____

☐ pleaded nolo contendere to count(s) _____
which was accepted by the court.

☒ was found guilty on count(s) 5s and 6s of the Superseding Indictment
after a plea of not guilty.

The defendant is adjudicated guilty of these offenses:

Title & Section	Nature of Offense	Offense Ended	Count
18 U.S.C. §§2252(a)(1) and 2252(b)(1)	Transportation of Child Pornography	10/22/2013	5s
18 U.S.C. §§2252(a)(2) and 2252(b)(1)	Sexual Exploitation of a Child - Distribution of Child Pornography	12/27/2013	6s
18 U.S.C. §§2252(a)(2) and (A)(4)(B)	Criminal Forfeiture Allegation	N/A	N/A

The defendant is sentenced as provided in pages 2 through 8 of this judgment. The sentence is imposed pursuant to the Sentencing Reform Act of 1984.

☐ The defendant has been found not guilty on count(s) _____

☒ Count(s) 1s, 2s, 3s, and 4s of the Superseding Indictment

☐ is ☒ are dismissed on the motion of the United States.

It is ordered that the defendant must notify the United States attorney for this district within 30 days of any change of name, residence, or mailing address until all fines, restitution, costs, and special assessments imposed by this judgment are fully paid. If ordered to pay restitution, the defendant must notify the court and United States Attorney of material changes in economic circumstances.

5/18/2018
Date of Imposition of Judgment

S/ RALPH R. BEISTLINE
Signature of Judge

Ralph R. Beistline, Senior United States District Judge
Name and Title of Judge

6/04/2018
Date

Appendix C

DEFENDANT: KALEB L. BASEY
CASE NUMBER: 4:14-CR-00028-01-RRB

IMPRISONMENT

The defendant is hereby committed to the custody of the United States Bureau of Prisons to be imprisoned for a total term of:

180 MONTHS

This term consists of 180 months on Counts 5s and 6s, to run concurrently.

☒ The court makes the following recommendations to the Bureau of Prisons:

The Court STRONGLY recommends the defendant serve his term of imprisonment in Indiana.

☒ The defendant is remanded to the custody of the United States Marshal.

☐ The defendant shall surrender to the United States Marshal for this district:

☐ at _____ ☐ a.m. ☐ p.m. on _____.

☐ as notified by the United States Marshal.

☐ The defendant shall surrender for service of sentence at the institution designated by the Bureau of Prisons:

☐ before 2 p.m. on _____.

☐ as notified by the United States Marshal.

☐ as notified by the Probation or Pretrial Services Office.

RETURN

I have executed this judgment as follows:

Defendant delivered on _____ to _____

at _____, with a certified copy of this judgment.

_____
UNITED STATES MARSHAL

By _____
DEPUTY UNITED STATES MARSHAL

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, Plaintiff, vs. KALEB LEE BASEY, Defendant.	4:14-cr-00028-RRB-SAO **REPORT AND RECOMMENDATION REGARDING DEFENDANT'S MOTION TO SUPPRESS FILED OCTOBER 4, 2016 (Dkt. 130)**

INTRODUCTION

Basey was indicted on three counts of Attempted Enticement of a Minor in violation of 18 U.S.C. § 2242(b) and one count of Receipt of Child Pornography in violation of 18 U.S.C. § 2252(a)(2).[1] The defendant, Kaleb Lee Basey (Basey), filed two Motions to Suppress at Dkts. 44 and 49, the Magistrate Judge addressed both in a Final Report and Recommendation (R & R) at Dkt. 110. The District Court judge adopted the Magistrate Judge's R & R at Dkt. 113.[2]

Basey obtained new counsel. New counsel filed the instant motion requesting that this court reconsider several of its Recommendations to the District Court judge made in Dkt. 110. Basey renewed his motion to suppress all fruits of law enforcement's search of his barracks room, custodial statements made to law enforcement after the unlawful search, and suppress all

[1] Original Indictment (Dkt. 2) was filed on December 16, 2014. A Superseding Indictment (Dkt. 101) was filed on March 17, 2016 charging Basey with three counts of Attempted Enticement of a Minor in violation of 18 U.S.C. § 2422(b), one count of Receipt of Child Pornography in violation of 18 U.S.C. § 2252(a)(2) and (b)(1), one count of Transportation of Child Pornography in violation of 18 U.S.C. § 2252(a)(1) and (b)(1), and one count of Distribution of Child Pornography in violation of 18 U.S.C. § 2252(a)(2) and (b)(1).

[2] A typographical error was noted in the District Judge's Order at Dkt. 113, it is discussed below and corrective action included as a recommendation.

evidence obtained from a subsequent U. S. District Court warrant[3] authorizing the FBI to search his electronics seized from his room. Basey supplemented his motion with an addendum.[4] The United States filed a response in opposition to the motion,[5] and Basey filed a reply in support of the motion.[6] Thereafter, the court issued an order from chambers directing additional briefing on proscribed questions of law from the United States, and the court invited Basey to respond in kind.[7] Both parties filed responsive briefs.[8]

ISSUES PRESENTED[9]

This Report and Recommendation primarily examines the following issues:

---

[3] This case included federal, state, and military warrants. Two of those warrants are at issue here. The first warrant was issued by a military magistrate who authorized a search of Basey's barracks room. The second warrant was issued by a U.S. District Court magistrate judge, approximately nine months after the military warrant, and authorized a search of the electronics seized from Basey's barracks room. For the reader's ease, the first warrant is herein referred to as "the military warrant" while the latter is referred to as "the federal warrant." Basey did not raise concerns and this R & R does not address the other warrants.

[4] Dkt. 135-1.

[5] Dkt. 139.

[6] Dkt. 142.

[7] Dkt. 149. The order informed the parties that the court rejected the United States' argument that Basey's instant motion must be reviewed under the doctrine of law of the case. (Citing, e.g., United States v. Smith, 389 F.3d 944, 949 (9th Cir. 2004) ("The law of the case doctrine is wholly inapposite to circumstances where a district court seeks to reconsider an order over which it has not been divested of jurisdiction.[ ]All rulings of a trial court are subject to revision at any time before the entry of judgment . . . The doctrine simply does not impinge upon a district court's power to reconsider its own interlocutory order provided that the district court has not been divested of jurisdiction over the order.")) This court instead construed Basey's motion as one for reconsideration. The parties were informed that the court would entertain Basey's motion de novo and provided the United States opportunity to respond to Basey's arguments.

[8] United States at Dkt. 152, Basey at Dkt. 156.

[9] As explained above, the court construes Basey's motion as one for reconsideration, since the issues presented have been previously raised and adjudicated. Any of the parties' arguments not addressed in this R&R which were addressed at Dkt. 110 remain undisturbed and unchanged.

1. Whether Basey's statement's to Agent Shanahan in the U.S. Army Criminal Investigation Division's (CID) office at Fort Wainwright, Alaska were tainted as fruits of the unlawful search of his barracks room, pursuant to a military search warrant and, if so, whether they must be suppressed.

2. If the federal warrant contained tainted information, whether a neutral magistrate would find probable cause to issue a warrant, without relying on any tainted evidence contained in the affidavit.

HISTORY OF ISSUES PRESENTED

This court previously found the search of Basey's barracks room to have been unlawful because the military warrant authorizing it lacked probable cause.[10] Basey was taken into custody and questioned by law enforcement shortly after the search. Basey was repeatedly advised of his rights under Article 31 of the Uniform Code of Military Justice by CID Agent Shanahan, and he voluntarily made several statements to law enforcement.[11] After the initial Report and Recommendation found that the search was unlawful, Basey objected to the Report and Recommendation on the grounds that his statements to Agent Shanahan were tainted fruit of the search and should be suppressed.[12] Basey did not proffer any argument in support of his

[10] Dkt. 110.

[11] Basey's earlier motion, as adjudicated by this court at Dkt. 110, sought suppression of various statements Basey made to law enforcement in various locations, at various times, and to various law enforcement personnel. The instant motion involves only the statements Basey made to Agent Shanahan in the CID interview room immediately following him being taken into custody. For the reader's ease, reference herein to "Basey's statements" refer specifically and only to those made in the CID interview room unless otherwise specified.

[12] Dkt. 97 at 4-7.

assertion as to taint, but included a cursory citation to U.S. v. Shetler,[13] the Ninth Circuit's cornerstone case on confessions potentially tainted by illegal searches. This court considered but rejected Basey's new argument, instead relying on the Ninth Circuit's holding in U.S. v. Green[14] which allows for an exception to the taint rule of Shetler. Basey, with new counsel, now embraces Shetler and offers additional argument, urging the court to do the same and suppress his post-search statements.

Basey's opening brief discussed Shetler but failed to address this court's earlier reliance on Green. His reply brief, however, and his later brief in response to this court's order, did. In Green, the court held that despite a confession's taint from an earlier illegal search, the confession was nonetheless admissible because the role of the illegally obtained evidence in inducing the confession was *de minimis* when the defendant had already been confronted with other legally obtained and significantly more inculpable evidence.[15] Basey argues that while the fact pattern in this case is similar to that of Green, the nature of the evidence Basey was presented with is too dissimilar to Green, and therefore this court should retract its reliance on Green and conduct its analysis under the default rules in Shetler.

Basey contrasts Green in two ways. First, he states that the electronics unlawfully seized from his room were far from *de minimis*, and were the "prime cause" of his confession that child pornography was on his computer.[16] Second, he argues that while law enforcement may have confronted him with other evidence that was legally obtained, none of that evidence was

[13] United States v. Shelter, 665 F. 3d 1150 (9th Cir. 2011).

[14] United States v. Green, 523 F.2d 968 (91h Cir. 1975).

[15] Green at 972.

[16] Dkt. 142 at 4.

indicative of child pornography, although indicative of other crimes. Basey concludes that under these circumstances, the illegally obtained evidence could not be *de minimis*.

The United States urges the court to affirm the ruling in its earlier R&R. The prime contention is that Green controls because the effect of the illegal search on Basey's confession to possession of child pornography was "at best *de minimis*."[17] The argument rests on an assertion that Basey was only confronted with the illegal search by an innocuous, unspecific statement made by Agent Shanahan to Basey that law enforcement would be "going through all [the defendant's] stuff and find[ing] everything."[18] This sole statement, it is argued, does not confront Basey with any illegally seized evidence from the unlawful search. Even if it did, the United States' position is that the confrontation was nonspecific and, when added to the "overwhelming quantity of lawfully obtained evidence relating to the defendant's pandering activities on Craigslist, such a single, generalized statement about 'going through all [the defendant's] stuff' is *de minimis* within the meaning of Green."[19] Finally, the United States concludes, even if Basey was confronted with the unlawful search at the time he made his statements, the search was sufficiently attenuated from those statements sufficient to remove any taint.[20]

Basey further argues that once this court suppresses the custodial statements made to Agent Shanahan, the court should then suppress evidence obtained from the subsequent federal warrant because "the weightiest evidence contained in the supporting affidavit was Basey's

---

[17] Dkt. 152 at 4.

[18] Dkt. 152 at 4, 6.

[19] Dkt. 152 at 5.

[20] Dkt. 152 at 9.

interrogation statements, including his confession to having child porn on his computer."[21] Once this court suppresses those statements, it must excise the statements from the affidavit presented to the U.S. Magistrate Judge and reassess whether probable cause existed. Basey argues the federal warrant will lack probable cause, the evidence obtained from the federal warrant is tainted, and thus that evidence must be suppressed.

The United States disagrees by contending that even if Basey's statements are suppressed and then excised from the probable cause analysis for the federal warrant, sufficient probable cause remained to support the federal warrant to search Basey's electronics for evidence of enticement of a minor and child pornography. The United States contends further that even if the warrant lacked probable cause to search the electronics for child pornography, sufficient probable cause remained to authorize the search for evidence related to solicitation of a minor.[22]

RECOMMENDATIONS

Upon due consideration of the arguments presented by the parties, and reconsideration of these issues, this court hereby recommends that:

1. Basey's renewed motion to suppress his statements made at the CID office to Agent Shanahan be GRANTED in part and DENIED in part; and

2. Basey's motion to suppress the evidence obtained from the search of his electronics be DENIED.

FINDINGS OF FACT[23]

[21] Dkt. 130 at 16.

[22] Dkt. 152 at 14.

[23] The Findings of Fact remain substantially unchanged from the elaborate findings made at Dkt. 110. They are reproduced here in full for convenience of the reader. Any alterations to the

The Investigation

A worker from the State of Alaska's Office of Children's Services contacted the investigation department of the Alaska State Troopers, the Alaska Bureau of Investigation (ABI), on January 15. 2014. The worker described an advertisement placed on Craigslist, an online forum where anyone can post advertisements. The posting, listed in the Fairbanks section, was located in a category of "Personals" and in the section labeled "Casual Encounters."[24] Most postings in "Casual Encounters" are of a sexual nature and seek a sexual encounter. It was originally posted January 15, 2014 at 9:46pm and modified on January 16, 2014 at 10:15pm.[25] The posting, Government Ex. 3, included text and a photograph of a young, clothed girl laying on a couch. The posting was titled "daughter share – m4w" and read:

> "any dads or moms want to share a daughter with me for the night? just gauging interest, must have a daughter. respond with torchat id if you got one. Fit, attractive, kinky, hung male here."[26]

The Alaska State Troopers sent an evidence preservation request to Craigslist, located in San Francisco, California, requesting them to preserve the Craigslist ad "4289756436 "daughter

---

FINDINGS OF FACT are in italics. A notable alteration is at page 19 where the court quotes more precisely the dialogue between Agent Shanahan and Basey in the interview room, extracted from Government Ex. 8, admitted at the evidentiary hearing. Immediately under that addition, the court also added additional quotation from Agent Shanahan's court testimony.

[24] Agent Shanahan believed the only reason one would post an ad in the "Casual Encounters" section of Craigslist would be to obtain sexual favors, sexual meet-ups, or establish other sexual contact.

[25] Many times in this case are described in the military format, however, this Report and Recommendation converted all times referenced to standard time format for convenience of the reader.

[26] Government Ex. 3.

share – m4w" (Fairbanks)."[27] Investigator Ramin Dunford (ABI) requested and received a search warrant from a State of Alaska Magistrate Judge.[28] The warrant and affidavit were admitted as Government Ex. 2 and 2a. Investigator Dunford identified the Internet Protocol (IP) address used to place the posting and then contacted the internet service provider for this IP address. General Communication Inc. (GCI), an internet service provider for Fairbanks and Fort Wainwright, gave Investigator Dunford the customer information for the customer utilizing the IP address at the date and time of the Craigslist posting. GCI identified the customer as Kaleb Basey, residing at 3442 Ile De France, Room 310A, Fort Wainwright, Fairbanks, Alaska[29] with a service activation date of August 23, 2013.[30] Investigator Hanson (ABI) contacted the Army Criminal Investigations Division (CID) at Fort Wainwright with this information. Investigator Hanson met with CID Agent Sean Patrick Shanahan. Agent Shanahan conducted a Department of Defense people search using the information provided by GCI. Agent Shanahan concluded that "Kaleb Basey" was in fact, Specialist Kaleb Basey, an active duty Army Soldier assigned to and residing on Fort Wainwright, Alaska. While the investigation was ongoing, ABI informed Agent Shanahan that Kaleb Basey placed another posting on Craigslist with similar characteristics and terminology used as in the first posting. This posting, listed in the Fairbanks

[27] Government Ex. 2.

[28] The warrant ordered Craigslist to provide account information and other details related to the user who authored the posting.

[29] Fort Wainwright, Alaska is an active duty military installation located adjacent to Fairbanks, Alaska.

[30] 3442 Ile De France is located on Fort Wainwright, Alaska. It is a military barracks building with multiple barracks rooms set up like a college dormitory. On the first floor, a Soldier, serving as the Charge of Quarters (CQ), is posted on duty and monitors who enters and exits the main entrance of the building.

section, was also located in a category of "Personals" and called "Casual Encounters." It was originally posted on January 17, 2014 at 5:30pm and then modified at 10:27pm. The posting, Government Ex. 4, included text and a photograph of a middle aged woman and a young girl. This picture was more sexually suggestive than the first; an adult female and a young girl, clearly under the age of eighteen, both clothed, but with the adult female's hand on the front the young girl's pants. The posting was titled "Mom with young daughter – m4w" and read:

> "I'm a good looking guy looking for a mom who has a young daughter she'd like to share with me for taboo fun. It's a lot warmer here in Alaska today."[31]

Agent Shanahan continued to work with Investigator Hanson on January 17, 2014. Agent Shanahan went to the building at 3442 Ile De France on Fort Wainwright. Knowing Basey lived on the third floor, Agent Shanahan walked through the hallway on the third floor with an electronic device to learn which wireless internet or 'wifi' networks were available.[32] Agent Shanahan walked by Basey's room, Room 310A, and stood outside his door.[33] Agent Shanahan picked up three different wifi sources, all of which were password protected. This led Agent Shanahan and the other investigators to conclude the person using the IP address was utilizing the internet through either a hard-line internet connection or password protected wifi. This discovery appeared to eliminate the possibility another person from another location

---

[31] Government Ex. 4.

[32] The hallway is an open area running the length of each floor which allows building residents to access their individual rooms, like a dorm. Even though this building is a military barracks, there are suites designed to accommodate two Soldiers, each suite has three rooms, a common area which accesses a door to each of the Soldier's private rooms for a total of three rooms.

[33] Agent Shanahan observed a placard on the wall next to the door to room 310A listing Basey's name, rank, and unit.

utilizing the IP address to post the advertisements.[34] A digital forensic examiner, working with Investigator Hanson, tried to send an email to the email address account attached to the Craigslist posting but there was no response.

The Military Warrant

In conducting his investigation, Agent Shanahan turned to seeking to search Building 3442, room 310A, Specialist Kaleb Basey's barracks room and felt the investigation was very urgent.[35] The procedures for obtaining a search authorization from a Military Magistrate under the Military Rules of Evidence differ from those under the Federal Rules of Criminal Procedure. Military Rule of Evidence 315(b)(1) defines an "authorization to search" as an "express permission, written or oral, issued by competent military authority to search a person or an area for specified property or evidence or for a specific person and to seize such property, evidence, or person."[36] Agent Shanahan contacted a Military Magistrate located at Joint Base Lewis-

[34] During this time, Agent Shanahan shared his information with Investigator Hanson and both were actively investigating.

[35] Agent Shanahan pointed to several details in the investigation, including their concern that Basey may actually have been physically seeking out children; that Basey's barracks were located approximately two miles from the nearest on-base family housing where children reside; the two advertisements listed in quick succession; the escalating lascivious nature of the photographs; and uncertainty about whether Basey had access to children.

[36] This court is not going to examine and opine on the differences in procedures, because the probable cause standard applies to both, and the appropriate inquiry is whether or not probable cause existed within the four corners of the underlying affidavit as required under United States v. Stanert, 762 F.2d 775, 778 (9th Cir.1985).

search using the terms "young" and "pre-teen." Basey admitted that that mother-daughter scenario excited him, but did not believe he would actually engage in a sexual encounter if offered. Basey described his email as "swingguy23@yahoo.com," and he also described "Torchat" as a place on-line to talk back and forth secretly.

Shanahan asked Basey a series of questions about computers, websites, passwords, usernames, and the like, and Basey answered his questions. Then, Agent Shanahan stated the following to Basey.

> *Um, is there anything else that I need to know about? Because I feel like we're being pretty honest with each other, pretty open, cuz, I'll tell you what I'm gonna do. I'm gonna go through all your stuff . . . I'm gonna go through all of it, I'm gonna find everything, good and bad; what else ... I mean, a bunch or porn, every guy's laptop in the fricken world. We delete our history but its still there, so what else are we gonna find on there? I'm just trying to prepare myself so I'm like, okay, this is all wrapped up, and all of a sudden kaboom. So . . .*[75]

Basey then confessed, "Um, yea, you'll find, some, I guess child porn."[76] *Immediately after Basey's statement, Agent Shanahan stopped his questioning and told Basey he would have to re-advise him of his rights. Agent Shanahan took a break, left the room, and provided water to Basey.*

Starting at 4:19am, Agent Shanahan advised Basey of his rights using another DA3881, Government Ex. 11. Agent Shanahan read Block A and told Basey he was suspected of

---

[75] *Government's Exhibit 8 at 4:07:50.* As noted above, italicized text is indicative of facts or analysis not included in the initial Report and Recommendation (Dkt. 110). At Docket 142, n.1, Basey identified that certain dialogue was missing from the video footage at Government Exhibit 8. The court has located the footage and included it herein.

[76] *Shanahan testified as follows regarding the exchange: "I told him we were going to be examining his -- all the evidence we took, his cell phone, his computer, all of that stuff. And I asked him, I said, is there anything else we're going to find on here, because I don't like being surprised. And it's a tool I use in the interview, as well, to just get it all on the table." Trans. at 92.*

FILED

SEP 23 2019

MOLLY C. DWYER, CLERK
U.S. COURT OF APPEALS

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. KALEB L. BASEY, Defendant-Appellant.	No. 18-30121 D.C. No. 4:14-cr-00028-RRB District of Alaska, Fairbanks ORDER

Before: TALLMAN, IKUTA, and N.R. SMITH, Circuit Judges.

Judge Ikuta has voted to deny the petition for rehearing en banc and Judge Tallman and Judge N.R. Smith so recommend.

The full court has been advised of the petition for rehearing en banc and no judge has requested a vote on whether to rehear the matter en banc. *See* Fed. R. App. P. 35.

Appellant's petition for rehearing en banc (Docket Entry No. 76) is denied.

Appendix E

18-30121

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

(Panel: Judge N.R. Smith, Tallman and Ikuta,
Memorandum Decision: August 14, 2019)

UNITED STATES OF AMERICA) Plaintiff-Appellee,)	No. 18-30121 DC No. 4:14-cr-28-RRB
v.)	
KALEB LEE BASEY) Defendant-Appellant.)	

ON APPEAL FROM THE JUDGMENT OF
THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

APPELLANT'S PETITION FOR REHEARING EN BANC

Kaleb Lee Basey
17753-006 Cardinal Unit
Federal Medical Center Lexington
P.O. Box 14500
Lexington, KY 40512-4500
Defendant-Appellant in Pro Se

Appendix F

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES **PAGE(s)**

CASES **PAGE(s)**

CASES **PAGE(s)**

STATUTES **PAGE(s)**

I. FRAP 35(b) Statement.

The defense respectfully asks this Court to grant en banc review under FRAP 35(b)(2) in this, the first case ever to present a United States Court of Appeals the following question of exceptional importance:

> Does the government's use of 18 U.S.C. § 2703(f)[1] to compel an internet service provider (ISPs) to warrantlessly preserve a private individual's emails amount to a search or seizure under the Fourth Amendment?

The government uses § 2703(f) to preserve hundreds of thousands of individual's electronically stored information (ESI) nationwide every year. The government may hold this information for months, with any showing of probable cause or exigency, before getting a warrant. Section 2703(f)'s use is increasing and shows no signs of stopping given the ever-increasing amount of information stored online. An en banc decision is warranted to curb the potentially massive abuses of 2703(f) and preserve the Fourth Amendment rights of Americans in the digital age. Also, another case currently before this Court, U.S. v. Perez, No. 18-30004, raises essentially the same

[1] Section 2703(f) requires ISPs to "take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process." 18 U.S.C. § 2703(f)(1). ISPs must retain the information for 90 days with the option to extend for another 90 days. § 2703(f)(2).

exceptionally important issue regarding 2703(f) and could be consolidated with Basey's case en banc.

II. Background

In February 2014, police send a 2703(f) to Yahoo! to preserve Basey's emails.[2] The government has conceded that Basey's emails were preserved by Yahoo!.[3] Nine months later a warrant was obtained for Basey's emails in November 2014.[4] Basey was charged by superseding indictment in March 2016,[5] and convicted on the basis of two preserved emails from his account.[6] A panel of this Court did not address Basey's 2703(f)-related suppression issue because it felt the district court did not abuse its discretion in denying Basey's attorney a continuance to address it in a suppression motion. App. Dkt. 70-1 (Memorandum Decision) at *2 no. 1.[7]

---

[2] [ER 695] (Government's Answer to Proposed Additional Motions) ("Records indicate that [a 2703(f)] letter was sent to Yahoo! by law enforcement in February 2014...[Basey's] content was held by Yahoo! and preserved by that private entity at the United States' request."). This excerpt constituted a judicial admission of fact by the government to Yahoo!'s preservation of Basey's email account which is binding on appeal. American Title Insurance Company v. Lacelaw Corp., 861 F.2d 224, 226 (9th Cir. 1988).

[3] App. Dkt. 51 (Appellee's Answering Brief) at 5 n.2 ("[T]he United States did not dispute below that the preservation request was sent to Yahoo.").

[4] [SER 133-139] (Yahoo! Search Warrant).

[5] [ER 711-17].

[6] [SER 188].

[7] This Court may still address Basey's 2703(f) issue even if it was not properly before the panel since it "has the authority and discretion to decide questions first

III. Warrantless Preservation of Private Information Pursuant to 2703(f) is an Exceptionally Important Issue.

Every year, law enforcement uses 2703(f) requests to effectively seize privately information in hundreds of thousands of online accounts. Here, the government admitted that it compelled Yahoo! to preserve Basey's emails before getting a warrant. Once the emails were preserved, Basey could no longer exclude the government from possessing his emails--the digital equivalent of his private papers and effects protected by the Fourth Amendment. This case is illustrative of a growing trend in the use of 2703(f) to covertly, collect information just in case police decide to get a warrant later on.

The use of 2703(f) raises grave constitutional concerns and has lead one Justice to ponder, "Can the government demand a copy of all your

---

raised in a petition for rehearing *en banc*." U.S. v. Hernandez-Estrada, 749 F.3d 1154, 1159 (9th Cir. 2013). Also, since the 2703(f) issue presents a constitutional issue, "[e]xception [to waiver] has frequently been made for constitutional questions, even if not raised on direct appeal." U.S. v. Schlesinger, 49 F.3d 483, 485 (9th Cir. 1994). Moreover, since the government made a judicial admission to Basey's emails being preserved by Yahoo!, this Court may at least decide whether the Fourth Amendment was implicated since this is a pure question of law. U.S. v. Flores-Payon, 942 F.2d 556, 558 (9th Cir. 1991) (outlining an exception for issues of pure law raised for the first time on appeal). The Court could then remand to address the reasonableness of any search or seizure and whether exclusion of evidence is appropriate.

emails...without implicating your Fourth Amendment rights?" Carpenter v. U.S., 138 S. Ct. 2206, 2262 (2018) (Gorsuch, J., dissenting). Justice Gorsuch's question is essentially the one raised by Basey for this Court's consideration en banc. The Fourth Amendment is implicated and an en banc decision will help clarify the law surrounding this exceptionally important issue.

A. The increasing, wideside, and unchecked use of 2703(f) to preserve private information underscores the importance of this issue.

This is not an isolated or occasional concern. The use of 2703(f) is staggering and on the rise. In the first half of 2018, Facebook received 57,000 preservation requests for 96,000 different accounts.[8] However, investigators never demonstrated any basis for their 2703(f) requests on almost 23,000 occasions during that time frame. In that same time frame, Google received 8,698 letters affecting 22,030 accounts.[9] From 2017 to 2018, both companies experienced between 20% and 30% increases in 2703(f) letters and affected accounts.

---

[8] Facebook, *Transparency Report: Government Requests (United States)*, https://perma.cc/TVV5-QYW9 (last visited Feb. 19, 2019).

[9] Google, *Transparency Report: Request for User Information (United States)*, https://perma.cc/MP98-8SCP (last visited Feb. 19, 2019).

Despite the prevalence of 2703(f) as an investigative tool, there is virtually no case law addressing it, likely owing to the covert nature of the request.[10] Since any mention of any 2703(f) requests may be inconspicuous in a defendant's discovery, it is essential that an authoritative en banc opinion be issued to highlight its importance to police, prosecutors, defendants, and the public.

"When requests for...information have become so numerous that the [ISP] must develop a self-service website so that law enforcement agents can retrieve user data from the comfort of their desks, we can safely say that 'such dragnet-type law enforcement practices' are already in use." U.S. v. Pineda-Moreno, 613 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of rehearing en banc) (my alteration). What was true 9 years ago is more so today where ISPs offer police websites with self-service 2703(f) requests forms.[11] This Court's en banc intervention is needed now to ensure that the Fourth Amendment does not become

---

[10] U.S. v. Rosenow, 2018 US Dist. LEXIS 198054, *32 (S.D. Cal. Nov. 2018); In the Matter of the Search of Premises Known as: Three Hotmail Email Accounts, No. 1-MJ-8036-DJW, 2016 WL 1239916, at *12 n.78 (D. Kan. Mar. 28, 2016) (noting that the case at issue was "the first time that the Court can remember the government indicating that it renewed its preservation requests" within the allotted 90 days).

[11] E.g., Rosenow, supra at *12 (describing Facebook's Law Enforcement Online Request System) (LEORS) for processing 2703(f) requests).

a dead letter as police accelerate their warrantless access to rich troves of digital papers and effects.

B. Section 2703(f) implicates Fourth Amendment rights making its use and misuse an issue of exceptional importance.

Section 2703(f) preservation may frequently violate Fourth Amendment rights given its widespread, arbitrary, and unchecked use. "[A]n email is a 'paper' or 'effect' for Fourth Amendment purposes."[12] Americans have possessory interests in their emails since they exclude others from them.[13] When the government compels an ISP to preserve emails, the ISP becomes a government agent.[14] Because the government interferes with one's right to exclude by its copying or preservation; it prevents exclusive possession, use, and disposition of those emails resulting in a meaningful interference with one's possessory interest--a seizure.[15] While privacy-based approaches may offer protection from

---

[12] U.S. v. Ackerman, 831 F.3d 1292, 1304 (10th Cir. 2016) (opinion by Gorsuch, J.)
[13] BLACK'S LAW DICTIONARY at 1284 (9th ed. 2009) (defining "possessory interest" as the "present or future right to exclusive use and possession of property:).
[14] U.S. v. Miller, 688 F.2d 652, 657 (9th Cir. 1982).
[15] U.S. v. Jacobsen, 466 U.S. 109, 113 (1984).

unreasonable searches,[16] an *en banc* property-based approach would fill in the gap to protect against unreasonable seizures of ESI.[17]

Additionally, a search also occurs as ISPs must intrude upon password protected accounts and emails to obtain and preserve the customers information for the government. See Florida v. Jardines, 596 U.S. 1, 11 (2013) ("when the Government obtains information by physically intruding on persons, houses, papers, or affects, a 'search' within the original meaning of the Fourth Amendment has undoubtedly occurred."); Ackerman, 831 F.3d at 1308 (trespass may occur by electronic means).

It cannot be stressed enough how important it is to address a 2703(f) seizure issue when it presents itself since it lacks any notice requirement. This makes it almost impossible to assert your possessory interests, once your emails or other ESI is preserved. It "strike[s] at the very heart of the interests protected by the Fourth Amendment."[18] Senders of emails may also retain possessory interests in

---

[16] E.g., U.S. v. Forrester, 512 F.3d 500 (9th Cir. 2008).

[17] See U.S. v. Jones, 625 F.3d 766, 770 (D.C. Cir. 2010) (Kavanaugh, J., dissenting from denial of rehearing en banc) (property-based Fourth Amendment challenge to GPS tracker installation "poses an important question and deserves careful consideration by the en banc court").

[18] U.S. v. Freitas, 800 F.2d 1451, 1456 (9th Cir. 1986).

their sent messages within a seized account. This could exponentially increase the number of people affected by 2703(f).

The lengthy preservation in this case violated Basey's Fourth Amendment rights. However, this court sitting en banc need only address the important threshold issue of whether the Fourth Amendment was implicated by 2703(f). The panel's refusal to address the exceptionally important issue is unfortunate, but has left a blank slate to write on. Courts have consistently condemned "stealthy encroachment"[19] by overzealous officers or permitted by judicial laxity. To further abstain from addressing the important issues in this case would be a disservice to tens if not hundreds of thousands of Americans.

C. Recent *en banc* and Supreme Court cases have recognized a need to reexamine traditional understandings of the Fourth Amendment in the digital age.

This Court and other Circuits sitting *en banc* have recognized the need to confront crucial questions regarding the Fourth Amendment in the digital age. See, e.g., U.S. v. Dreyer, 804 F.3d 1266 (9th Cir. 2015) (en banc) (addressing electronic searches and seizures conducted by military personnel); U.S. v. Comprehensive

[19] U.S. v. Page, 302 F.2d 81, 83 (9th Cir. 1962). See also Olmstead v. U.S., 277 U.S. 438, 479 (1928) ("the greatest dangers to liberty lurk in insidious encroachment by men of zeal.").

Drug Testing, Inc. ("CDT III"), 621 F.3d 1162 (9th Cir. 2013) (per curiam) (procedures for issuing warrants ESI); U.S. v. Cotterman, 709 F.3d 952 (9th Cir. 2012) (en banc) (addressing border searches of digital devices); U.S. v. Ganias, 824 F.3d 199 (2d Cir. 2016) (en banc) (addressing retention of ESI seized by warrant); U.S. v. Davis, 785 F.3d 498 (11th Cir. 2015) (en banc) (addressing search and seizure of cell site location information) "CSLI")).

The issues present here regarding 2703(f) are arguably more important than those presented in previous *en banc* decisions. While not every investigation involves the military, border crossings, search warrants, or requests for CSLI; a majority of cases involving digital information will likely involve 2703(f). See Microsoft Corp. v. U.S., 855 F.3d 53, 63 & n.4 (dd Cir. 2017) (Cabrares, J., dissenting from denial of rehearing en banc) (arguing that an en banc review is appropriate where it involves "an essential investigative tool used thousands of times a year [in] important criminal investigations around the country"). Every warrant for a social media or email account or CSLI is likely tied to a previous 2703(f) request as government agencies encourage this as a best practice. Every search of a digital device will likely yield online accounts police can preserve with 2703(f). It is difficult to overstate the importance of addressing the constitutional implications of 2703(f).

At least thrice in recent terms the supreme court has confronted crucial questions regarding the Fourth Amendment in the digital age. See Carpenter v. U.S., 138 S. Ct. 2206 (2018) (warrants for CSLI); Riley v. California, 134 S. Ct. 2473 (2014) (warrant required to search cell phone seized incident to lawful arrest); U.S. v. Jones, 132 S. Ct. 945 (2012) (tracking car with a GPS device is a Fourth Amendment search). This case presents an important step in the ongoing effort to reconcile enduring Fourth Amendment principles with the reality of a new digital world. Given the panel's decision to not address Basey's 2703(f) issue, the supreme court's decision to address the important issues here is far from inevitable *en banc* review is appropriate here because this is "the exceptional case that is an unlikely candidate for supreme court resolution." John M. Walker, Jr., *forward*, 21 Quinnipiac L. Rev. 1, 14 (2001).

IV. Conclusion.

The Executive Branch has made a bid for unrestricted power to secretly seize our private information by exploiting §2703(f). Without judicial guidance police will continue their unchecked intrusions under the statute. This is an issue of great, long-term importance to business and ordinary citizens alike requiring *en banc* review to protect the constitutional rights of Americans in the digital era.

Kaleb Lee Basey
Kaleb Lee Basey
Defendant-Appellant in Pro Se

CERTIFICATE OF SERVICE

I hereby certify that on this 24th day of August, 2019, I mailed Appellant's Petition for Rehearing *En Banc* and a copy of the panel opinion to the clerk of court for the United States Court of Appeals for the Ninth Circuit.

Kaleb Lee Basey
Kaleb Lee Basey
Defendant-Appellant in Pro Se

Molly Dwyer, Clerk of Court
Office of the Clerk
United States Court of Appeals
Ninth Circuit
P.O. Box 193939
San Francisco, California 94119-3939

federal warrant does not satisfy the particularity requirement. It therefore is in violation of the Fourth Amendment. Furthermore, the presentation of illegally obtained evidence precludes an application of the good faith exception to the exclusionary rule. United States v. Vasey, 834 F.2d 782, 789 (9th Cir. 1987).

This argument was previously advanced by Basey. See Addendum To Motion To Suppress, at Page 2. It is believed that the Court has not addressed it.

3. Motion To Suppress Yahoo Warrant:

On November 20, 2014, this Court granted search warrant 3:14-mj-49, which commanded the seizure of specified Yahoo e-mail account records reflecting activity during specified periods of time. This warrant should be suppressed for the following reasons:

First, the warrant suffers from the same defects, and relies on the same suppressed statements, that invalidates the federal warrant for the search of the devices.

Second, the execution was unreasonable. Information in Yahoo accounts may be deleted by the owners of the accounts. On information and belief, Yahoo received a preservation letter in February, 2014. This made it impossible for the owners of the designated accounts, including Basey, to delete material from their accounts. A search warrant ordering the seizure of the contents of the designated accounts was issued approximately nine months later. This was an unreasonable amount of time to interfere with Basey's possessory right to his account. Thus, suppression is required.

Third, the Yahoo warrant is overbroad. As a result of a grand jury subpoena, the Government knew precisely when e-mail communications were sent and received regarding the CraigsList postings. Yet, authority was granted to search e-mail accounts over broad swaths of time. For instance, the warrant authorized the seizure of information contained in Basey's account for a period of nearly six months. Yet, for large portions of that period, there was no probable cause to believe that the account contained evidence of the violation of any

Rex Lamont Butler
and Associates, Inc.
745 W. 4th Ave.,
Suite 300
Anchorage, Alaska
99501

907-272-1497
907-276-3306 (f)

evidence of crimes will be found in a particular place." Illinois v. Gates, 462 U.S. 213, 236 (1983). The defendant's claim that the Yahoo! search warrant was lacking is without merit.

iii. There Was No Violation of the Stored Communications Act.

The defendant also argues that the search of his Yahoo! account was unreasonable due to the delay between its preservation pursuant to a request filed by law enforcement in January 2014 under the authority of Stored Communications Ac (SCA), 18 U.S.C. § 2703(f), and the account's search in November 2014. However, this argument fails to understand the mechanics of preservation requests made under federal law.

The SCA requires electronic communications services like Yahoo! to "take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process." 18 U.S.C. § 2703(f). Retention of such records can be accomplish through a preservation letter. Records indicate that such a letter was sent to Yahoo! by law enforcement in February 2014.

At no time prior to the search of his account was law enforcement in possession of any content from the defendant's Yahoo! account. Rather, that content was held by Yahoo!, and preserved by that private entity at the United States' request. It cannot be argued by virtue of the preservation letter that the United States was in possession of any material.

Furthermore, Yahoo! cannot be considered a government agent. This is necessarily so because the SCA requires a search warrant, court order, or consent of the account holder prior to disclosure of any contents preserved pursuant to a

preservation letter. Were Yahoo! a government actor, no such further order or consent would be needed.

In addition, preservation does not equal obstruction. The defendant offers nothing to support his argument that there was any interference with his possessory interest. Nonetheless, even if such denial of access occurred, it was not the result of any government action, but rather, by virtue of the defendant's violation of Yahoo!'s terms of service that prohibit use of the service to engage in illegal activity.

The United States is unable to locate any cases, reported or otherwise, that address the claim made by the defendant. This is remarkable given the fact that the SCA has been in existence since 1986, and speaks to the fundamental misunderstanding the defendant possesses about preservation letters and their operation. The service of a preservation letter to a private company is not a government seizure of evidence. Absent any seizure by the United States, there can be no 4th Amendment violation.[1]

iv. The Search Warrant Was Not Overbroad.

The defendant complains that the Yahoo! search warrant was overbroad because it sought information for a period of six months, from August 1, 2013, through January 22, 2014. It is true that the United States sought information

[1] Congress authorized preservation of evidence. Congress also authorized civil remedies against private actors for any party aggrieved by a violation of the statute. See 18 U.S.C. § 2707. If the defendant has any objection to the preservation of records from his account, this is where his remedy lies.

AO 93 (Rev. 12/09) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

District of Alaska

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)*	)	
Yahoo Email Accounts Identified in Attachment A	)	Case No. 3:14-mj-00349~~-KJM~~ KFM

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of Alaska
(identify the person or describe the property to be searched and give its location):

See Attachment A

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized):*

See Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before December 2, 2014
(not to exceed 14 days)

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge Kevin F. McCoy, or the on-duty magistrate
(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☐ for _____ days *(not to exceed 30)*.

☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 11-20-2014 2:45 pm

/s/ Kevin F. McCoy
United States Magistrate Judge
Signature Redacted

City and state: Anchorage, Alaska

KEVIN F. McCOY, United States Magistrate Judge
Printed name and title

Appendix I

AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
3:14-mj-00349 KJM F	11/20/14 @ 5:40pm	N/A

Inventory made in the presence of :

N/A

Inventory of the property taken and name of any person(s) seized:

One CD-R containing requested records received on 1/23/2014.

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 2/18/15

Executing officer's signature

SA Idlene Gooden

Printed name and title

Subscribed, sworn to, and returned before me this date.

Signature Redacted

KEVIN F MCCOY
U.S. Magistrate Judge

Date

Attachment A
Location to Be Searched

The location to be searched is information associated with the following YAHOO e-mail accounts:

1. swingguy23@yahoo.com,

2. [redacted]
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.
14.
15.
16.

(hereinafter "SUBJECT ACCOUNTS") that is stored at premises owned, maintained, controlled, or operated by Yahoo, Inc., headquartered at 701 First Ave, Sunnyvale, California 94089, fax number (408) 349-7941.

Attachment B
Items to Be Seized

For the Yahoo email accounts

1. swingguy23@yahoo.com,

2. [redacted]
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.
14.
15.
16.

(hereinafter "SUBJECT ACCOUNTS") and any other screen names associated with these accounts, the following records maintained by Yahoo, Inc.:

1. All subscriber information for the SUBJECT ACCOUNTS, including:

   a. names, email addresses, and screen names;

b. addresses;

c. detailed billing records or records of session times and durations;

d. length of service (including start date) and types of service utilized;

e. telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

f. the means and source of payment for such service (including any credit card or bank account number).

2. For the date ranges listed below, all transactional information for the SUBJECT ACCOUNTS, including:

a. logs of Internet Protocol ("IP") address connections, including dates, times, and time zones, and any ANI information made available to Yahoo, Inc.;

b. address books;

c. buddy lists; and

d. account history, including contacts with Yahoo, Inc. support services and records of actions taken online by the subscriber or by Yahoo, Inc. support staff in connection with the service.

3. For the date ranges listed below, the contents of electronic or wire communications held in accounts of the SUBJECT ACCOUNTS, including:

a. all electronic or wire communications with a minor or any person purporting to be a minor, or claiming to have access to a minor, or that otherwise involve the enticement of a minor to engage in sexual activity

for which any person can be charged with a criminal offense (including e-mail text, attachments, and embedded files) in electronic storage by the PROVIDER, or held by the PROVIDER as a remote computing service (if any), within the meaning of the Stored Communications Act;

b. all photos, files, data, or information in whatever form and by whatever means they have been created or stored relating to a minor, or individuals claiming to have access to a minor, or that otherwise involve the enticement of a minor to engage in sexual activity for which any person can be charged with a criminal offense.

4. The date ranges sought in this search warrant are as follows:

1. swingguy23@yahoo.com - August 1, 2013 to January 22, 2014

2. [redacted]
3.
4.
5.
6.
7.
8.
9.
10
11
12

4257212221?

A. I do.

Q. And what was that posting title?

A. It was the same, "Fuck while watching kinky porn - M4W."

Q. And now we've got an "RE," colon in front of that. Do you know what that RE, colon, stands for?

A. Regarding a reference.

Q. Okay. So swingguy23@yahoo.com e-mail replies to the Esther Crabb e-mail. What does Swingguy23 write?

A. He writes -- it's right above what we just read -- "Would you be into watching some of this?"

Q. Now, with that e-mail, were there any images attached?

A. There were.

Q. And generally speaking, can you describe what image was attached to the swingguy23@yahoo.com e-mail?

A. It's an image of two prepubescent children with what appears to be an adult male penis between them.

Q. And was the file name for that image the file name that's indicated there on the bottom of the screen, 1388053260175.jpeg?

A. That's correct.

MR. REARDON: Can we scroll down, please?

BY MR. REARDON:

A. This is a copy of one of the e-mails that I received from Yahoo from the swingguy23@yahoo.com e-mail.

Q. And what is the date on Exhibit 13?

A. December 22nd -- I'm sorry.

October 22nd, 2013.

Q. And what is the "from" account on this e-mail?

A. From H M Swingguy -- H M, and then swingguy23@yahoo.com.

Q. And what is the "to" account -- or the "to" address, rather?

A. Swingguy23@yahoo.com.

Q. And does this e-mail contain an attachment?

A. It does.

Q. And that attachment is a photograph?

A. It is.

MR. REARDON: Your Honor, the Government moves to admit Exhibit 13 into evidence.

MR. BUTLER: 13 is the e-mail itself, right?

MR. REARDON: Yes, it is.

MR. BUTLER: Okay. No objection to that, Judge.

THE COURT: 13 will be received.

(Exhibit No. 13 admitted.)

BY MR. REARDON:

Q. And then 13A is in the binder there in front of you. What is 13A?

A. 13A is just a redacted version of the picture on the e-mail.

Q. So it's the same e-mail in 13, with the picture redacted?

A. That's correct.

MR. REARDON: Your Honor, the Government moves to admit and seeks to publish Exhibit 13A.

MR. BUTLER: No objection.

THE COURT: Is that the redacted or the unredacted?

MR. REARDON: 13A is the redacted copy, Your Honor.

THE COURT: Okay. It will be received.

(Exhibit No. 13A admitted.)

(Pause.)

MR. REARDON: So let's just highlight the top portion here.

BY MR. REARDON:

Q. So looking at Exhibit 13A, what's been put up on the screen, again, the "from" address is swingguy23@yahoo.com?

A. Yes.

Q. And the "to" address is the same address?

image, but I don't think we need do that. I think we can just publish the e-mail and it would accomplish the same thing. We'd ask for the admonition to be read.

THE COURT: Okay. She hasn't described what it is yet.

BY MR. REARDON:

Q. Special Agent Goeden, can I ask you to describe in general terms what the image that's identified by the long series of letters and numbers starting with "Matrix" and ending in 75e.3.jpeg, what that attachment shows?

A. Sure. This is an image of a prepubescent child, a toddler, with an adult male penis in her mouth. You can see the room. There's a crib in the background as well.

MR. REARDON: Thank you, Your Honor. We ask now permission to publish.

THE COURT: Okay. Very well. And I'll read the admonition.

You're about to see an image that the Government alleges contains a visual depiction of a minor engaged in sexually explicit conduct. This image is being shown only to assist you in determining whether the Government has met its burden to prove the defendant guilty of all the elements of the charge against him.

A. Correct.

Q. In your training and experience, have you seen instances in which individuals have sent e-mails to themselves?

A. I have.

Q. And based on your training and experience, in what situations have you seen this occur?

A. I have seen it occur in order to move an image from one device to another. So for example, if I have an image on my computer, but I also want to have it on my cell phone, I can e-mail it to myself and it will be on my cell phone, or I'll have access to it on my cell phone.

Q. Now, the image that is attached to Exhibit 13, 13A, is there a file name for that exhibit?

A. There is.

Q. I'm sorry, for that attachment?

A. Yes.

Q. Can you read that file name into the record, please?

A. I can. It's a long one. "Matrix TXRI 745 DFW onion_131022110431 JAL_332 A68435A 3682341191EED 6FE 097 5E3.jpg."

MR. REARDON: Your Honor, the Government moves to publish Exhibit 13. I have a 13B, which is just the

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