FILED

JAN 18 2022

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. 21-35554 D.C. Nos. 4:20-cv-00015-RRB 4:14-cr-00028-RRB-1 District of Alaska, Fairbanks ORDER

Before: PAEZ and HURWITZ, Circuit Judges.

This appeal is from the denial of appellant's 28 U.S.C. § 2255 motion and subsequent Federal Rule of Civil Procedure 59(e) motion. The request for a certificate of appealability (Docket Entry No. 3) is denied because appellant has not shown that "jurists of reason would find it debatable whether the [section 2255 motion] states a valid claim of the denial of a constitutional right and that jurists of reason would find it debatable whether the district court was correct in its procedural ruling." *Slack v. McDaniel*, 529 U.S. 473, 484 (2000); *see also* 28 U.S.C. § 2253(c)(2); *Gonzalez v. Thaler*, 565 U.S. 134, 140-41 (2012); *Miller-El v. Cockrell*, 537 U.S. 322, 327 (2003); *United States v. Winkles*, 795 F.3d 1134, 1143 (9th Cir. 2015).

Any pending motions are denied as moot.

DENIED.

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 **AMENDED** **ORDER DENYING PETITION FOR RELIEF PURSUANT TO § 2255** **(Dockets 294, 295, 296)**

Defendant filed a Motion Under 28 U.S.C. § 2255 to Vacate, Set Aside, or Correct his sentence of 180 months in prison, with lifetime mandatory supervised release, for transportation and distribution of child pornography.[1] The government has opposed the motion,[2] and Defendant has replied.[3] This Court previously issued an Order Denying Petition for Relief Pursuant to §2255 and Denying Pending Motions as Moot.[4] At Defendant's request,[5] to which the Government did not respond, this Amended Order

[1] Dockets 294, 295, 296.
[2] Docket 316.
[3] Docket 334-4.
[4] Docket 357.
[5] Docket 360.

denying the § 2255 petition clarifies issues that Defendant felt were inadequately addressed in the prior Order.[6]

I. BACKGROUND

A comprehensive summary of the facts of this case may be found in the Magistrate Judge's May 9, 2017, Final Report and Recommendation.[7] Relevant points on the timeline are as follows:

- **January 15, 2014** – The Alaska Bureau of Investigation began an investigation into a Craigslist advertisement which appeared to be posted by an adult male looking for sexual encounters with young girls.[8]
- **January 17 & 18, 2014** – The Army Criminal Investigations Division ("CID") obtained a military search warrant and searched Defendant's room, seizing electronic devices.[9]
- **February 2014** – A preservation letter was sent to Yahoo to preserve the email account at issue pursuant to the Stored Communications Act, specifically 18 U.S.C. § 2703(f).[10][11]
- **November 20, 2014** – The FBI obtained a federal search warrant for the Yahoo email account.[12]
- **December 16, 2014** – A Grand Jury indicted Defendant for Attempted Enticement of a Minor and Receipt of Child Pornography.[13]
- **March 17, 2016** – A Grand Jury returned a Superseding indictment which added counts for Transportation of Child Pornography and Sexual Exploitation of a Child – Distribution of Child Pornography in violation of

[6] To the extent that Docket 357 dismissed the motions at Dockets 342, 343, 344, 349, 355, and 356, those issues will not be revisited here, and Docket 357 remains the final order on those motions.

[7] Docket 160 at 7–26.

[8] Docket 110 at 6.

[9] Docket 110 at 11–12.

[10] Docket 171 at 3.

[11] The Stored Communications Act addresses the obligation of email service providers to preserve electronic evidence at the request of a government entity. 18 U.S.C. 121 §§ 2701–2712.

[12] Docket 171 at 3.

[13] Docket 2.

18 U.S.C. § 2252.[14] These counts related primarily to evidence recovered from the Yahoo email account.

- **May 19, 2016** – Appointed FPD counsel moved to withdraw.[15] CJA counsel was appointed a few days later.[16]

- **October 4, 2016** – CJA counsel filed a Motion to Suppress "all evidence secured by executing the military search warrant; all statements made by Basey during the course of his custodial interrogation; and all evidence secured by executing the federal search warrant."[17] This motion ultimately was granted in part and denied in part on May 31, 2017, when this Court suppressed a portion of Defendant's statements, but denied the motion to suppress the evidence obtained from the search of Defendant's electronics.[18]

- **June 28 and July 7, 2017** – Appointed CJA counsel moved to continue trial, seeking permission to file a motion to suppress the Yahoo emails seized pursuant to the federal warrant.[19] This motion was denied following a hearing and further briefing.[20] The Court found that "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."[21]

- **November 16, 2017** – Defendant filed a *pro se* motion to suppress, wherein he **invoked** the Posse Comitatus Act and argued that his Yahoo emails should have been suppressed.[22] This motion also was denied.[23]

- Prior to trial, the government dismissed the original four counts and proceeded solely on the two counts arising primarily from the search of the Yahoo account.[24] Defendant was convicted by a jury.[25]

---

[14] Docket 101.

[15] Docket 114. *See also* Docket 295, alleging that counsel stated her strong belief that such a motion lacked merit and would be unsuccessful.

[16] Docket 123.

[17] Docket 130.

[18] Docket 165.

[19] Dockets 166, 171.

[20] Dockets 170, 171, 172, 173.

[21] Docket 173.

[22] Docket 194.

[23] Docket 200.

[24] *See* Docket 207.

[25] Docket 214.

After his conviction, which was upheld on appeal,[26] Defendant filed a 67-page memorandum in support of his *pro se* § 2255 Petition.[27] He alleges that both appointed trial counsel were ineffective under *Strickland v. Washington,*[28] because they failed to move to suppress his Yahoo emails, and that he was prejudiced by their failure to do so because the emails formed the sole basis of his conviction.[29]

On September 30, 2020, the Court provisionally appointed the Federal Public Defender to assist Defendant with his § 2255 Petition, and appointed counsel entered an appearance shortly thereafter.[30] Despite being represented by counsel, Defendant continued to file *pro se* motions,[31] and his counsel was permitted to withdraw in light of Defendant's expressed desire to proceed *pro se*.[32] Accordingly, the Court considered the § 2255 Petition as originally filed.[33]

II. DISCUSSION

Defendant alleges that his attorneys "were ineffective because they failed to file a motion to suppress his Yahoo emails," suggesting that his counsel "lacked a tactical basis" for failing to do so, and that their grounds for such failure were "unreasonable." Defendant himself filed a *pro se* motion to suppress the same emails prior to trial,[34] which was denied first on the record, and then in writing

---

[26] Docket 267.
[27] Docket 296.
[28] 466 U.S. 668 (1984).
[29] *Id.*
[30] Dockets 319, 320.
[31] *See* Docket 327 (Motion for Injunction); Docket 329 (Motion to file *pro se* Reply).
[32] Dockets 331, 334, 335, 336.
[33] Dockets 294, 295, 296.
[34] *See* Docket 194 at 14–19.

following a Motion for Reconsideration.[35] He now spends a dozen pages expounding on his reasoning that "Yahoo's [terms of service] did not destroy Basey's expectation of privacy in his emails,"[36] that his first trial counsel "abandoned her duty to research the law and make a good faith argument to extend, modify, or reverse existing law,"[37] and that his second trial counsel was negligent for failing to file a timely motion to suppress.[38] But as this Court has previously explained[39]:

> In order to prevail [under *Strickland*], the defendant must show both that counsel's representation fell below an objective standard of reasonableness, . . . and that there exists a reasonable probability that, but for counsel's unprofessional errors, the result of the proceeding would have been different. . . . Where defense counsel's failure to litigate a Fourth Amendment claim competently is the principal allegation of ineffectiveness, **the defendant must also prove that his Fourth Amendment claim is meritorious and that there is a reasonable probability that the verdict would have been different absent the excludable evidence in order to demonstrate actual prejudice.**[40]

Defendant's § 2255 Petition, therefore, hinges on the validity of his argument that had he persuaded either of his attorneys to file a motion to suppress his emails, such a motion

---

[35] Dockets 198, 199, 200. Defendant argued there that the emails were fruits of the poisonous tree, regardless of any privacy interest he had in them.

[36] Docket 296 at 4–10.

[37] *Id.* at 10–13.

[38] *Id.* at 13–16.

[39] Docket 306.

[40] *Kimmelman v. Morrison*, 477 U.S. 365, 374–75 (1986) (emphasis added), citing *Strickland v. Washington*, 466 U.S. 668, 688 (1984).

would have been successful. Only if such a motion would have been granted could the Court grant Defendant's various discovery motions, or find his lawyers were ineffective under *Strickland* for failing/refusing to file such a motion. Defendant does not allege ineffective assistance of counsel on any other grounds. Despite Defendant's voluminous briefing, Defendant's arguments fail.

This Court was aware of the issue of suppression of Defendant's emails prior to trial and, after holding a hearing on the matter, declined to entertain more briefing.[41] At that time, Defendant's CJA attorney raised one of the arguments that Defendant asserts here.[42] Defendant complains that he did not have a "'full and fair' opportunity to litigate the reasonable probability of the suppression motion's success" at that juncture.[43] While the Court's decision not to allow further briefing on the email issue may preclude collateral estoppel, the briefing currently before the Court is adequate to evaluate the issue.

Section II of Defendant's § 2255 petition, entitled "A motion to suppress Basey's emails would have been meritorious," presents four theories, containing a total of 13 sub-sections, seeking to satisfy the threshold question. Defendant argued that his Yahoo emails should have been suppressed because:

> (1) "The FBI's decision to seek the warrant for Basey's emails and the magistrate's decision to issue the warrant were tainted by the prior illegalities of the ASD and CID" as fruit of the poisonous tree;[44]

---

[41] Docket 173.

[42] Docket 171 at 3, arguing that that the nine-month delay from the date of the preservation letter to Yahoo until the warrant was issued was an "unreasonable amount of time to interfere with Basey's possessory right to his [email] account."

[43] Docket 334-4 at 34.

[44] Docket 296 at 18–33 (containing two subsections).

(2) "The warrant for Basey's emails lacked particularity **and was** overbroad;"[45]

(3) "The execution of the Yahoo warrant was overbroad;"[46]

(4) "The 9-month warrantless seizure of Basey's emails under a 2703(f) letter was unreasonable."[47]

A. Fruit of the Poisonous Tree

Defendant argues that the seizure of his electronic devices during the search of his barracks room was unlawful, and that therefore the November 2014 warrant to search his Yahoo emails was tainted as fruit of the poisonous tree because the Yahoo warrant was based on information gained from the "illegal search of his barracks room and devices."[48] Defendant is wrong. As the Magistrate and this Court previously and repeatedly have explained, although this Court held that the search of Defendant's *room* lacked probable cause, it specifically found that the federal search warrant to search the seized *electronic devices* was lawful.[49] The legal search of those devices led law enforcement to seek a warrant for Defendant's email.

---

[45] *Id.* at 33–42 (containing six subsections).

[46] *Id.* at 42–44.

[47] *Id.* at 44–66 (containing five subsections and four sub-subsections).

[48] *Id.* at 18–33.

[49] *See* Docket 110 at 23, 44–49, 63–64. The Magistrate Judge and this Court each made this determination twice. The Magistrate Judge issued a Final Report and Recommendation Regarding Motion to Suppress Evidence and Statements, recommending in part that "the continued retention of the electronic devices seized from Basey's room on January 18, 2014 was lawful, and **the evidence resulting from the search under the federal warrant issued on November 3, 2014 should not be suppressed.**" Docket 110 at 44 (emphasis added). This Court adopted the Report and Recommendation. Docket 113. Defendant then renewed his Motion to Suppress, Docket 130, which the Magistrate interpreted as a Motion for Reconsideration. Docket 149. Upon reconsideration, **the Magistrate *again* recommended that Defendant's motion to suppress the evidence obtained from the search of his electronics be denied.** Docket 160. This Court again followed the recommendation of the Magistrate Judge. Docket 165.

Accordingly, the issuance of the warrant for Defendant's email was not "tainted by the prior illegalities." Defendant's argument fails.

B. Particularity and Overbreadth/Search of Email Account

Defendant's next two arguments suggest that the warrant for his Yahoo emails "lacked particularity" and that both the warrant and its execution were "overbroad."[50] He complains that although "the government had down-to-the-minute information as to when certain emails were sent to Basey's email account," and that it "could have used that information to target specific emails," the government instead sought copies of Defendant's Yahoo emails in bulk for a six month period.[51]

Defendant relies heavily upon an earlier published opinion which found that a search warrant application for the *entire content* of multiple targeted email accounts was overbroad when a more specific date range was available.[52] But the limitations in the search warrant here were specifically tailored to target the relevant time period and subject matter. The affiant here sought emails from Defendant's email address from "the date of the first advertisement through one week after the last email that was sent through the Craigslist servers."[53] Further, the affidavit

[50] Docket 296 at 33–44.

[51] *Id.* at 40.

[52] *In re Search of Google Email Accounts identified in Attachment A*, 92 F. Supp. 3d 944, 951 (D. Alaska 2015). (Finding an application for the entirety of email accounts from Gmail overbroad, when a more specific date range was available).

[53] Docket 172-1 at 30, ¶ 27 (Affidavit of Special Agent Goeden in support of Search Warrant).

specifically limited the request to "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."[54] Defendant has provided no authority that indicates that the parameters of the search warrant application here were overbroad or lacked particularity such that they violated the Fourth Amendment. Nor is there any evidence that the search warrant was not consulted during its execution, or that Defendant was prejudiced in any event.

Next, Defendant complains that the terms of the search warrant affidavit did not specifically seek emails between himself and a particular "me.com" email address, and that it was "ultimately the emails that the affidavit didn't seek that were used to convict Basey."[55] Having concluded that the warrant was valid, the Court takes judicial notice that the emails Defendant referenced here involved Defendant telling the recipient about his proclivity toward sexual acts involving "5 to 15-year-old[s]."[56] Such emails were precisely the type of emails requested in the warrant. Defendant's argument that the warrant for his emails was overbroad and lacked particularity, as well as his complaint that the warrant's execution was overbroad, are without merit.

---

[54] Docket 172-1.
[55] Docket 296 at 36.
[56] *See* Docket 261 at 139 (trial transcript of government's closing statement).

C. Seizure under 18 U.S.C. §2307(f) Preservation Letter

The Stored Communications Act generally prohibits "'providers' of communication services from divulging private communications to certain entities and/or individuals."[57] Section 2703 addresses the obligation of email service providers to preserve electronic evidence at the request of a government entity. It reads, in relevant part:

> (f) Requirement **To Preserve Evidence.—**
> **(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.[58]

Defendant argues at length about § 2703.[59]

1. Yahoo was not a "government agent"

Defendant complains that although the intent of § 2703(f) is to *temporarily* preserve electronic files while law enforcement can obtain a warrant, entities such as Yahoo routinely preserve information for much longer periods of time, beyond the 180 days contemplated by the statute, because they have a "monetary incentive" to preserve

---

[57] *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 900 (9th Cir. 2008), rev'd on other grounds.

[58] 18 U.S.C. § 2703(f).

[59] At Docket 360, Defendant complains that this Court's prior order focused primarily on Defendant's §2703(f) argument. However, this section of Defendant's § 2255 Petition comprised a full third of Defendant's argument.

emails under § 2706 which reimburses ISPs for their compliance with the Stored Communications Act "regardless of when legal process arrives."[60]

However, Defendant does not argue that § 2703 is unconstitutional.[61] Rather, Defendant argues that by preserving the emails, Yahoo became a government agent, and by exceeding the 180 day requirement Yahoo, as a government agent, engaged in an unreasonable search and seizure in violation of the Fourth Amendment.[62] Despite Defendant's extensive briefing, this premise is unsupported by the caselaw, as explained in the government's briefing.[63]

2. Initial seizure of emails was reasonable

Defendant also argues that "the government did not have probable cause to initially search and seize [his] Yahoo account and emails under the 2703(f) letter."[64] A preservation request pursuant to § 2703(f) notifies the online provider to "take all necessary steps to preserve records" of an account. The request does not interfere with the use of the account or entitle the Government to obtain information without further legal process. Moreover, in the absence of a warrant, the Fourth Amendment permits the seizure of property, pending issuance of a warrant to

[60] Docket 334-4 at 38. Section 2706 reads in relevant part: "a governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information."

[61] Docket 334-4 at 36.

[62] *Id.* at 36–45.

[63] Docket 316 at 22–27.

[64] Docket 359 at 2, citing Docket 296 at 52–54.

examine its contents, if probable cause exists and "if the exigencies of the circumstances demand it . . . ."[65] Defendant argues that there was neither probable cause nor exigent circumstance.[66]

Defendant's reasoning is difficult to follow, but he seems to argue that because he did not admit that his emails contained child pornography, there was no probable cause to seize his emails.[67] But a defendant's admission is not required to show probable cause. Probable cause is a "totality of the circumstances" test and means "'fair probability,' not certainty or even a preponderance of the evidence."[68] Defendant's admission that "the initial preservation was ***at most supported by reasonable suspicion***,"[69] while not a relevant standard, does not weigh in his favor.

Moreover, Defendant's argument again relies on his position that the search of his devices was "illegal," which, as discussed above, was not the case. Additionally, the Magistrate already has performed this analysis in the Report and Recommendation at Docket 160, wherein he concluded that even in the absence of the tainted statements, there was probable cause to search Defendant's electronic

---

[65] *United States v. Place*, 462 U.S. 696, 701 (1983).

[66] Docket 296 at 53–54.

[67] Defendant argued that "the government did not have probable cause to initially search and seize Basey's Yahoo account and emails under the 2703(f) letter. The only reason the CID preserved Basey's account was because they thought Basey had used the account 'to view/distribute child [pornography].' But Basey never said he used the email account for that purpose." Docket 296 at 53. He then admits that although the topic of child pornography "came up," during his interrogation, his statement was later suppressed by the Court. *Id.*

[68] *United States v. Gourde*, 440 F.3d 1065, 1069 (9th Cir. 2006)

[69] Docket 296 at 61.

devices.[70] The same analysis applies to establish probable cause for the preservation letter.

Defendant also argues that there was no exigency. However, the very nature of emails, which easily can be deleted by a user, is one reason § 2703(f) letters remain in use. Despite criticism of § 2703(f), the use of § 2703(f) letters remains a law enforcement standard.[71]

3. Continued preservation was reasonable

The Court is unpersuaded by Defendant's argument that the period of delay between the § 2703(f) preservation letter and the warrant was "astronomical,"[72] or that the investigators failed to exercise "diligence in obtaining the warrant."[73] Under the circumstances, the Court cannot find this delay sufficiently long to defeat the warrant or to otherwise infringe on any constitutional right.

Finally, with respect to Defendant's argument regarding the unfairness of the common practice of retaining materials beyond 180 days in order to get reimbursed by the government, the Stored Communications Act does *not* provide an exclusion remedy for nonconstitutional violations. Section 2708 states specifically that § 2707's civil cause of

[70] Docket 160 at 42–43.

[71] *See* Armin Tadayon, PRESERVATION REQUESTS AND THE FOURTH AMENDMENT, 44 SEAULR 105 (Fall, 2020).

[72] Docket 296 at 57–58.

[73] *Id.* at 60–61.

action and § 2701(b)'s criminal penalties "are the only judicial remedies and sanctions for nonconstitutional violations of this chapter."[74]

III. CONCLUSION

Defendant alleges ineffective assistance of counsel because counsel declined (or in the case of CJA counsel, delayed) filing a motion to suppress the emails that formed the basis of the charges against him. Even with the additional arguments articulated in the § 2255 briefing, the Court would not have granted a motion to suppress the emails, which was the only grounds upon which Defendant asserted ineffective assistance of counsel.

The Order at Docket 357 is VACATED IN PART with respect to the § 2255 Petition, as addressed herein. Having concluded that Defendant would not have prevailed on a suppression motion, the various discovery motions[75] therefore must be denied as addressed at Docket 357, which remains final as to those motions, and the Petition for relief under § 2255 is DENIED.

IV. CERTIFICATE OF APPEALABILITY

Finally, because Defendant has failed to make a substantial showing of the denial of a constitutional right, and reasonable jurists could not find otherwise, the Court declines to grant a Certificate of Appealability pursuant to 28 U.S.C. § 2253(c).

---

[74] 18 U.S.C. § 2708; *See United States v. Smith*, 155 F.3d 1051, 1056 (9th Cir. 1998) (finding that if a searched voicemail message is subject to the Wiretap Act then suppression is an available remedy for any violation, but "[i]f the voicemail message at issue is subject to the strictures of the Stored Communications Act, then suppression is not an available remedy.").

[75] Dockets 342, 343, 344, 349, 355, 356.

IT IS SO ORDERED this 13th day of April, 2021, at Anchorage, Alaska.

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

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA,
Plaintiff,

v.

Case Number 4:20-CV-00015-RRB
4:14-CR-00028-RRB

KALEB LEE BASEY,
Defendant.

JUDGMENT IN A CIVIL CASE

DECISION BY COURT. This action came to trial or hearing before the court. The issues have been tried or heard and a decision has been rendered.

IT IS ORDERED AND ADJUDGED:

THAT defendant's application for post-conviction relief [28 U.S.C. § 2255] is dismissed. The Court declines to grant a Certificate of Appealability pursuant to 28 U.S.C. § 2253(c).

APPROVED:

Ralph R. Beisline

Ralph R. Beistline
Senior United States District Judge

Date April 13, 2021

Brian D. Karth
Clerk of Court

Suzannette David-Waters
(By) Deputy Clerk

JMT2255 – rev. 1-13-15

FILED

JAN 31 2022

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. 21-35554 D.C. Nos. 4:20-cv-00015-RRB 4:14-cr-00028-RRB-1 District of Alaska, Fairbanks ORDER

Before: SILVERMAN and CHRISTEN, Circuit Judges.

Appellant's motion for reconsideration (Docket Entry No. 8) is denied. *See* 9th Cir. R. 27-10.

No further filings will be entertained in this closed case.

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

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

KALEB LEE BASEY, Petitioner,	)	No. _____
vs.	)	STATEMENT OF FACTS IN SUPPORT OF §2255 MOTION
UNITED STATES OF AMERICA, Respondent.	)	

A. The military search warrant and preservation of Basey's Yahoo account under 18 U.S.C. §2703(f).

On January 17, 2014, Army Criminal Investigation Division (CID) agents Sean Shanahan and Heather Rodgers along with Alaska State Trooper (AST) Kirsten Hansen were investigating the posting of an ad on the Fairbanks, Alaska, Craigslist website that they believed was a solicitation of

minors for sex.[1] The ad was traced to Kaleb Basey.[2] That night, Agent Shanahan obtained a military warrant to search Basey's barracks room for child pornography.[3] This warrant was later deemed constitutionally invalid by this Court.[4]

Basey's computer and iPhone were illegally seized from his barracks room around midnight on January 18, 2014, by the AST and CID.[5] Basey was arrested and taken to CID headquarters where Agent Shanahan induced a tainted confession from Basey using the illegally-seized property.[6]

The AST took custody of Basey's property the next day and performed digital forensic examinations of the devices.[7]

---

[1] Dkt. 160 at 7-8. "Dkt." refers to filings in Basey's criminal case. "App. Dkt." refers to filings from Basey's direct appeal of his criminal case, No. 18-30121.

[2] *Id.*

[3] *Id.* at 10-15; Dkt. 45-1 (military warrant).

[4] Dkt. 110 at 36.

[5] Dkt. 160 at 17; Dkt. 278-1 (CID property custody document).

[6] Dkt. 160 at 22, 30-39.

[7] *Id.* at 25-26; Dkt. 80 at 102 (Evid. Hrg. Tr.); Exh. 5 (AST Supplementary Report).

On January 25, 2014, Basey went to the Noel Wien public library in Fairbanks, Alaska, and deleted every email in his swingguy23@yahoo.com email account and then deleted the account itself.[8]

On February 6, 2014, a CID report indicates that they intended to preserve Basey's swingguy23@yahoo.com account because it was believed to have been used "to view/distribute child pornography."[9] On February 7, 2014, Agent Shanahan sent a preservation letter under 18 U.S.C. §2703(f) to Yahoo for Basey's email account.[10] When Yahoo receives 2703(f) letters, it creates a "snapshot" which is "a copy of all the contents of a user's Yahoo Mail account at a given moment in time."[11] Even deleted emails that have not yet been removed from Yahoo's servers are preserved as well.[12] Deleted accounts and

---

[8] Exh. 47 (Basey Decl.) ¶4; Exh. 4 (Bates 624/Yahoo IP log).

[9] Exh. 1 (Bates 1886/CID Agent's Activity Summary).

[10] *Id.*; Dkt. 172 at 9 (government admits "such a letter was sent to Yahoo! by law enforcement in February 2014").

[11] Exh. 9 (Yahoo's Response to Petitioner Russell Knagg's Special Interrogatories to Yahoo!, Inc., *Knaggs v. Yahoo, Inc.*, No. 5:15-mc-80281-PSG, ECF No. 13-1 at 30 (N.D. Cal. Jan. 16, 2016)).

[12] *Id.*

emails on Yahoo's servers normally remove themselves completely from the server within 40 days in the normal course of business.[13]

On February 11, 2014, Yahoo sent the CID a confirmation that Basey's emails had been preserved.[14] On February 20, 2014, CID Supervising Agent Heriberto Rodriguez stated: "Ok so we preserved [Basey's] account. We are pending the results of the forensic exams to support [probable cause] for a warrant."[15] Despite asking an AUSA if they had enough probable cause to get a warrant for Basey's emails,[16] the CID never obtained Basey's emails with a warrant.

B. The illegal search of Basey's devices triggers the FBI's involvement.

On May 7, 2014, AST computer technician Jeff Mills began his search of Basey's computer finding child pornography and "several emails of interest documenting the defendant's previous posting of a Craigslist advertisement

---

[13] Exh. 44 (email from Yahoo service representative to Loretta Gaines dated Nov. 5, 2019); Exh. 10 (Printout of Yahoo's Data Storage Policy) ("If you ask Yahoo to delete your Yahoo account, in most cases your account will be deactivated and then deleted from our user registration database in approximately 40 days....").

[14] Exh. 1 (Bates 1886/CID Agent's Activity Summary).

[15] Exh. 2 (Bates 1887/CID Agent's Activity Summary).

[16] Exh. 3 (Bates 1888-89/CID Agent's Activity Summary).

seeking a minor for sexual purposes."[17] Prior to this, AST investigator Albert Bell had illegally searched Basey's iPhone finding "messages where Basey requested sex with 'young' females."[18]

According to CID Agent Shanahan, "the way we were able to *move forward* was what we found on the digital evidence"—Basey's devices.[19] After discovering evidence during the illegal search of Basey's devices, the AST and CID contacted the FBI at the end of July 2014 to bring them into the loop.[20] At meetings held on July 25 and 30, 2014, between the CID, AST, and the FBI; the FBI was fully briefed on what was found on Basey's devices.[21] On August 12, 2014, the FBI was given a copy of the digital forensic examination (DFE) of Basey's devices.[22]

The FBI, however, did not obtain information regarding the initial January 2014 Craigslist posting until sometime in August 2014.[23] As of

---

[17] Exh. 5 (AST Supplementary Report 5/7/2014).

[18] *Id.* (AST Supplementary Report 2/7/2014).

[19] Dkt. 80 at 102, LL 11-17 (Evid. Hrg. Tr.) (emphasis added).

[20] *Id.* at 104, LL 18-22.

[21] *Id.* at 105, LL 6-12; Exh. 6 (Bates 1897-98) (CID AAS).

[22] *Id.* at 107, LL 1-3; Dkt. 278-1 (CID property custody document showing FBI Agent Baron Lambert received the discs on August 12, 2014).

[23] Dkt. 261 at 39, LL 6-10 (Trial Day 2 Tr.).

August 26, 2014, the FBI had searched the illegally-obtained DFE discs and "identified all the child porn images, [and] other content and briefed the U.S. attorney."[24] The FBI also sent a copy of the DFE disc to the National Center for Missing and Exploited Children (NCMEC) to have them search the disc as well.[25] The NCMEC is a government entity.[26]

On October 30, 2014, Craigslist sent the FBI additional information linked to Basey in response to a grand jury subpoena.[27]

C. The Yahoo affidavit and search warrant for Basey's emails.

Several things are notable about FBI Jolene Goeden's November 20, 2014, affidavit in support of the Yahoo search warrant:

- She does not mention a December 2013 Craigslist posting titled "fuck while watching kinky porn."
- She does not mention an email address called esthercrabb@me.com.

---

[24] Exh. 6 (Bates 1900/CID Agent's Activity Summary).

[25] Exh. 7 (Bates 222-24).

[26] *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016) (opinion by Gorsuch, J.).

[27] Dkt. 172-1 at 20-25, ¶21 (Yahoo Search Warrant Aff.); Exh. 8 (additional Craigslist information).

- She says she wants only "communications *between* Basey and the other [listed] email accounts."[28]
- She does not say she wants emails from Basey to himself.
- She does not describe or list any alleged child pornography.
- Despite knowing about the contents of copies of Basey's Yahoo emails on his devices, she did not include that information in her affidavit.[29]

Several things are notable about the Yahoo search warrant and its attachments:

- The warrant does not state a specific offense.
- The warrant seeks all of Basey's emails, not just the ones "*between* Basey and the other email accounts."[30]

Yahoo responded to the warrant on February 15, 2015, by supplying a disc containing what is likely to be the preserved snapshot of Basey's account.[31] The FBI searched Basey's entire email account, not just those "*between* Basey and the other email accounts," listed in the affidavit.[32]

D. Basey's first attorney refuses to file a motion to suppress his emails.

---

[28] *Id.* at 30, ¶27 (emphasis and alteration added).
[29] Exh. 5 (AST Supplementary Report 5/7/14).
[30] *Id.*
[31] Dkt. 172-1 at 2 (Yahoo Warrant Return).
[32] Dkt. 172-1 at 30, ¶27 (emphasis added).

Basey was indicted on December 16, 2014, with six Counts unrelated to his email account.[33] These counts would ultimately be dismissed before trial.[34] Basey's first counsel, M.J. Haden initially declined to file a motion to suppress his emails because (1) the government was not relying on the emails for the charges at this time and (2) she stated that Basey lacked an expectation of privacy and standing in his emails.[35]

About a year later, in early 2016, Haden told Basey that the government was planning to file a superseding indictment with charges related to his Yahoo emails.[36] Basey asked Haden to confirm the source of the emails and told Haden he had deleted all of his emails on his Yahoo account and the account itself on or about January 25, 2014.[37] Basey again asked Haden to file a motion to suppress his emails and she declined again citing his lack of an expectation of privacy and standing.[38] Basey asked Haden to

---

[33] Dkt. 160 at 1 n. 1.

[34] Dkt. 252 (pro nunc tunc dismissal of charges); Dkt. 257 at 1 (judgment noting dismissal).

[35] Exh. 47 (Basey Decl.) ¶3.

[36] Exh. 47 (Basey Decl.) ¶4.

[37] *Id.*

[38] *Id.*

identify a case that said people have no expectations of privacy in their emails.[39] Haden replied that *Smith v. Maryland*[40] and *United States v. Miller*[41] hold that information disclosed to third parties lacks privacy, hence no Fourth Amendment standing.[42] Basey said that that did not sound right and he would do his own research into the matter.[43] Notably, Haden did not consider the possibility that Basey's emails could be challenged as fruits of the poisonous tree which obviates the need for a privacy or possessory interest in the poisonous fruit.[44]

The following list is a summary of emails Basey caused to be sent to Haden trying to convince her to file a motion to suppress his emails:

- *February 14, 2016*: Basey urges Haden to challenge the additional Craigslist ads as fruits of the poisonous tree.[45]

---

[39] *Id.*

[40] 442 U.S. 735 (1979).

[41] 425 U.S. 435 (1976).

[42] Exh. 47 (Basey Decl.) ¶4.

[43] *Id.*

[44] Exh. 47 (Basey Decl.) ¶16.

[45] Exh. 11 (February 14, 2016, email to Haden).

- *February 22, 2016*: Basey provides Haden with three cases[46] that explicitly say one may have an expectation of privacy in emails.[47]

- *March 9, 2016*: Basey provides two more cases supporting his theory that the additional Craigslist ads can be challenged as fruits of the poisonous tree.[48]

- *March 11, 2016*: Basey makes an analogy to *United States v. Place*[49] saying, "The fruits of the FBI and AUSA's efforts, like the dog's reaction [in *Place*], must be suppressed as fruits of the poisonous tree."[50]

- *March 22, 2016*: Basey informs Haden about the landmark email privacy case *United States v. Warshak*.[51]

At this point, Basey began focusing more on the merits of a motion to suppress his emails since he established that Haden was incorrect about lacking privacy and standing.

- *March 24, 2016*: Basey highlighted the Yahoo warrant's lack of particularity and overbreadth, "The attachments to the warrant do not specify any specific offenses" and "executing agent[s]...would not be

---

[46] *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008); *United States v. Cioffi*, 668 F. Supp. 2d 385, 390 n.7 (E.D.N.Y. 2009); and *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 905 (9th Cir. 2008).

[47] Exh. 12 (February 22, 2016, email to Haden).

[48] Exh. 13 (March 9, 2016, email to Haden).

[49] 462 U.S. 696 (1983).

[50] Exh. 14 (March 11, 2016, email to Haden).

[51] Exh. 15 (March 22, 2016, email to Haden) (citing *United States v. Warshak*, 631 F.3d 266, 286-88 (6th Cir. 2010)).

informed to search certain email exchanges between certain accounts at certain times."[52]

- *March 27, 2016*: Basey observes that the number of potential offenses covered by the warrant may vary greatly given its lack of definitions and specificity.[53]

- *March 30, 2016:* Basey tells Haden that the preservation of his email account under 2703(f) amounted to a seizure and he mentioned a law review article by Orin S. Kerr that supported this.[54]

- *March 31, 2016*: Basey stresses the overbreadth of the warrant in comparison to the affidavit which only sought "communications between Basey and the other email accounts."[55]

- *April 2, 2016*: Basey notes that the Yahoo warrant "did not incorporate the affidavit," thus the affidavit could not cure a lack of particularity in the warrant.[56]

At some point in April, Haden met with Basey and expressed some interest in challenging the Yahoo warrant's lack of particularity.[57] Basey referenced her interest in an email dated April 10, 2016:

> I do like what you were saying about the ambiguity in the attachments. In addition to that point I want you to argue that the government exceeded the scope of the

---

[52] Exh. 16 (March 24, 2016, email to Haden).

[53] Exh. 17 (March 27, 2016, email to Haden).

[54] Exh. 18 (March 30, 2016, email to Haden).

[55] Exh. 19 (March 31, 2016, email to Haden).

[56] Exh. 20 (April 2, 2016, email to Haden).

[57] Exh. 47 (Basey Decl.) ¶5.

> affidavit by looking at emails other than what was allowed by the affidavit.
>
> Another issue I want you to raise in the email motion pertains to the seizure of information in the Yahoo...account that occurred pursuant to the 2703(f) request.[58]

On April 16, 2016, Basey sent Haden a 5-page draft of a motion to suppress the Yahoo emails on the basis of the unreasonably long seizure of his emails under 2703(f).[59] It was around this time that Haden began trying to convince Basey that Yahoo's privacy policy (not its terms of service (TOS)) would doom any motion to suppress his emails.[60] Haden was mere weeks away from retirement—though she did not tell Basey this—and was looking for an easy way out of her obligations to Basey.[61] Despite Haden's negativity, Basey still persisted on sending emails challenging the privacy policy issue,[62] that the good faith exception did not apply to the preservation of his emails,[63]

---

[58] Exh. 21 (April 10, 2016, email to Haden).

[59] Exh. 22 (April 16, 2016, email and draft motion to Haden).

[60] Exh. 47 (Basey Decl.) ¶6.

[61] *Id.* ¶7.

[62] Exh. 23 (April 18, 2016, email to Haden).

[63] *Id.*

and that the warrant was overbroad.[64] Basey also expressed his distrust of Haden during a phone call, stating that she had already misled him once by not knowing that reasonable expectations of privacy attach to emails.[65] Haden's response to this was if he did not trust her, then fire her.[66]

So he did.[67] But only after making a final plea for her to file his motion to suppress his emails, to which Haden said words to the effect:

> Mr. Basey, you do *not* have the moral high ground....
> Do you really think these judges would understand what you're asking me to file?....Would you like me to sell them a bridge too?....I'm not going to debate you about this....
> You can always file for ineffective assistance of counsel against me later on....[68]

On June 2, 2016, Rex Butler was appointed as Basey's CJA counsel.[69] Since the Superseding indictment was issued on March 17, 2016, Butler still

---

[64] Exh. 24 (April 27, 2016, email to Haden).

[65] Exh. 47 (Basey Decl.) ¶8.

[66] *Id.*

[67] *Id.* ¶10.

[68] *Id.* ¶9.

[69] Dkt. 121.

had time to file a *timely* motion to suppress Basey's emails.[70] But he ultimately would not.

E. Basey's second counsel fails to file a *timely* motion to suppress his emails.

Rex Butler has been an attorney since October 1978.[71] Butler was aware of the suppression issues Basey wanted addressed as well as his disagreement with Haden. As Butler said to the Ninth Circuit, "*one of the reasons* we were ultimately appointed CJA counsel and previous counsel withdrew" was because "Basey...believes that he is the smartest person in the room."[72] Despite knowing that Basey's case was an electronic search and seizure case, he took it on despite later admitting "I don't know a doggone thing about computers, other than to push a few buttons."[73] As it turns out, Butler did not know about court rules and meeting deadlines either. In fact, the Ninth Circuit censured Butler for repeatedly failing to follow its rules.[74]

---

[70] Dkt. 101 (Superseding Indictment).

[71] *United States v. Piers*, No. A00-104CR(HRH), 2005 U.S. Dist. LEXIS 43645, *10 (D. Alaska Oct. 21, 2005).

[72] App. Dkt. 16 at 2 (emphasis added).

[73] Dkt. 260 at 45 (Trial Tr.).

[74] App. Dkt. 79 *available at* 2019 U.S. App. LEXIS 26300 (9th Cir. Aug. 29, 2019).

Nevertheless, Basey still did his due diligence in trying to get Butler to file a motion to suppress his Yahoo emails. The following list is a summary of emails Basey caused to be sent to Butler trying to convince him to file the motion to suppress:

- *June 7, 2016*: Basey sends a draft motion to suppress the Yahoo emails on particularity and overbreadth grounds.[75]
- *July 17, 2016*: Basey suggests the difference between the scope of the Yahoo affidavit and Attachment B to the warrant may be due to alteration of the Attachment B after the warrant was issued.[76]
- *August 2, 2016*: Basey again invokes a poisonous fruits theory stating "the Yahoo search warrant was a product of the illegal searches...."[77]
- *September 5, 2016*: Basey states that the recently decided Ninth Circuit case *Grand Jury Subpoena v. Kitzhaber*[78], lent support to the Yahoo warrant being overbroad.[79]
- *September 6, 2016*: Basey alerts Butler to *United States v. Lustig,*[80] stating that the case provided "grounds for challenging the seizure of content information on the Yahoo account for over 6 months pursuant to 2703(f)...."[81]

---

[75] Exh. 26 (June 7, 2016, email to Mike Rhodes and Butler).

[76] Exh. 27 (July 17, 2016, email to Butler).

[77] Exh. 28 (August 2, 2016, email to Butler).

[78] 828 F.3d 1083 (9th Cir. 2015).

[79] Exh. 29 (September 5, 2016, email to Butler).

[80] *United States v. Lustig*, 830 F.3d 1075 (9th Cir. 2016).

[81] Exh. 30 (September 6, 2016, email to Butler).

But Butler did not challenge Basey's emails, instead Buler focused on attacking Haden's failure to argue that Basey's interrogation statements at the CID were tainted:

> Mr. Basey had a right to *effective assistance of counsel.* Any review of the discovery in this case inexorably leads to the conclusion that the issue of whether the confession was tainted by an illegal search must be litigated. Yet, Basey's counsel failed to litigate that issue in any meaningful manner.[82]

Unfortunately, the same could be said of Butler's handling of Basey's case with regards to the Yahoo emails. Basey sent a series of emails to Butler in June and July of 2017 discussing the need to file a motion to suppress his emails.[83] Had Butler simply "Googled" the term "2703(f)" he would have found an article by law professor Orin S. Kerr on challenging preservation letters as Fourth Amendment seizures.[84] Butler just did not want to put forth the effort and it showed.

---

[82] Dkt. 142 at 5.

[83] Exh. 31 (June 3, 2017, email to Butler); Exh. 32 (June 6, 2017, email to Butler); Exh. 33 (June 12, 2017, email to Butler); Exh. 34. (June 21, 2017, email to Butler); Exh. 35 (June 25, 2017, email to Butler); Exh. 36 (July 1, 2017, email to Butler); Exh. 37 (July 1, 2017, 8:54 pm email to Butler); Exh. 38 (July 2, 2017, email to Butler).

[84] Exh. 35 (citing Orin S. Kerr, *The Fourth Amendment and Email Preservation Letters*, Washington Post (Oct. 28, 2016) *available at* https://wapo.st/3czFcKe).

At a hearing on July 7, 2017, Butler claimed to have lost his notes regarding additional suppression issues that Basey wanted to raise.[85] Despite being past the pretrial motion deadline, Butler failed to show any good cause for untimely filing, e.g. Haden's refusal to file the motions. Afterall, Butler claimed to be aware that "*one of the reasons*" he was appointed was due to Basey's firing of Haden for refusing to file a motion to suppress his emails.[86] Instead, Butler cited his associate's retirement and the fact that Basey had identified additional meritorious suppression issues.[87] But this neglected the fact that Basey told Butler about the suppression issues, and Butler should have known about the issues, months beforehand.

This court ordered briefing on the additional suppression issues,[88] the parties submitted briefing,[89] and this Court denied the motion to continue trial to address the issues.[90]

---

[85] Dkt. 170; Exh. 47 (Basey Decl.) ¶13.

[86] App. Dkt. 16 at 2 (emphasis added).

[87] Dkt. 166.

[88] Dkt. 170.

[89] Dkt. 171 (Basey's memorandum); Dkt. 172 (Gov's memorandum).

[90] Dkt. 173 (Order denying continuance).

F. Trial and Appeal: Butler's failure to file a motion to suppress Basey's emails is part of a pattern of negligence.

On December 11, 2017, the government dismissed 4 of the 6 Counts of the Superseding Indictment hours before trial.[91] Two of Basey's preserved emails were used to convict him on the remaining Counts.[92]

Basey emailed a draft acquittal motion to Butler on December 19, 2017.[93] Butler had until December 26, 2017—14 days after conviction—to file the acquittal motion.[94] Butler, however, *untimely* filed the motion on January 4, 2018.[95] A side-by-side comparison of Basey's draft and Butler's filing shows that Butler simply copied and pasted the entire document.

Basey wrote his appeal brief in March 2018 and had his fiancée email it to Butler.[96] Despite having this material available to him, it took Butler until

---

[91] Dkt. 252.

[92] Dkt. 261 at 88 (Day 2 Trial Tr.) (evidence for distribution of child pornography Count); *id.* at 98-100 (evidence for transportation of child pornography Count).

[93] Exh. 39 (Dec. 19, 2017, email to Butler with draft acquittal motion).

[94] Fed. R. Crim. P. 29(a).

[95] Dkt. 217.

[96] Exh. 47 (Basey Decl.)¶14.

April 15, 2019—over a year later—to file an opening brief that was a 90% copy-and-paste of Basey early drafts.[97]

Ninth Circuit Rule 10-3.2(d) requires transcripts to be ordered within 21 days of the filing of the notice of appeal. Basey's notice of appeal was filed on May 30, 2018.[98] Butler submitted an *untimely* transcript request on August 22, 2018—83 days later.[99]

All told, the Ninth Circuit issued 7 orders finding Butler in non-compliance with its rules.[100] Butler would blame his problems on Basey, ie., saying Basey "ha[s] little or no insight regarding others" and "needs to keep his britches on."[101] And he would blame his underlings at his office.[102] Which, in retrospect, seems reasonable given that his secretary made the comment, "I forgot how particular the 9th Circuit is."[103]

---

97 App. Dkt. 47.

98 Dkt. 254.

99 Dkt. 259.

100 App. Dkts. 6; 8; 14; 22; 25; 35; 46.

101 App. Dkt. 16.

102 App. Dkt. 82.

103 Exh. 42 (Jan. 3, 2019, email from Butler's office).

The Ninth Circuit would ultimately rule that good cause had not been shown for the untimely request to reopen motion practice to address the additional suppression issues.[104] But Basey had still tried to show Butler to argue good cause as late as February 2019:

> If the appeals court would need further justification, i.e., good cause, I submit that my former-attorney (M.J. Haden) was ineffective for not raising these claims when I asked her to do so. In fact, this is why she withdrew herself from my case. She also did not know that well-established case law provided Fourth Amendment protection for emails further underscoring her inaptitude.[105]

Instead, Butler did not argue good cause in the opening brief or the reply. At oral argument Butler simply said, "it was a complex case."[106] It was obvious Butler had to argue something more than that. Even Professor Orin S. Kerr's cursory glance at Basey's district court files led him to say:

> I don't know if [Kaleb] can still appeal it [the 2703(f) issue]. This is an issue that ordinarily his attorneys would have been able to answer. I am not his lawyer, but it's potentially *a very serious problem*.[107]

---

[104] *United States v. Basey*, 784 Fed. Appx. 497, 498-99 (9th Cir. Aug. 5, 2019).

[105] Exh. 43 (Feb. 10, 2019, email to Butler with attachment).

[106] Oral Argument at 13:30, United States v. Basey (No. 18-30121), *available at* https://bit.ly/38wVOPE.

[107] Exh. 47 (Nov. 5, 2018, email from Orin S. Kerr).

And a very serious problem it was. But it doesn't take a law professor or even a lawyer to know that missing a court deadline is not good. And that was something Butler had serious issues with in this case.

Declaration

I, Kaleb Lee Basey, declare under penalty of perjury that the foregoing is true (or believe can be proved to be true) and correct.

Executed on April 11, 2020 at Lexington, KY.

Kaleb Lee Basey

Kaleb Lee Basey

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 . . . ."); *United States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir.1986) ("[S]urreptitious searches and seizures of intangibles strike at the very heart of the interests protected by the Fourth Amendment."); *Katz*, 389 U.S. at 353; *Berger v. New York*, 388 U.S. 41, 54–60 (1967) (telephone conversations); *United States v. Biasucci*, 786 F.2d 504, 509–10

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CONCLUSION

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

Date: February 19, 2019

Respectfully submitted,

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

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

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

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

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

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

Date: February 19, 2019

/s/ Jennifer Stisa Granick
Jennifer Stisa Granick

CERTIFICATE OF SERVICE

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

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

Date: February 19, 2019

/s/ Jennifer Stisa Granick
Jennifer Stisa Granick