# MODEL MOTION TO SUPPRESS CONTENTS OF AN INTERNET ACCOUNT BASED ON UNLAWFUL PRESERVATION UNDER 18 U.S.C. § 2703(f)

Version 4.0, February 28, 2023

Professor Orin Kerr, UC Berkeley Law School
E-mail: orin@berkeley.edu

This motion to suppress may be filed when the contents of an Internet account were preserved under 18 U.S.C. § 2703(f) before the government obtained a warrant to disclose the account contents under § 2703(a). The motion explains why preservation is a Fourth Amendment seizure that requires probable cause or at least reasonable suspicion. Because the government ordinarily uses § 2703(f) without any particularized suspicion, the contents of the account must be suppressed as a fruit of the unlawful preservation seizure.

For additional details about this argument, please read the law review article on which this draft motion is based: Orin S. Kerr, *The Fourth Amendment Limits of Internet Content Preservation*, 65 St. Louis U. L.J. 753 (2021). The article explains what Internet preservation is, how it works, and how the Fourth Amendment limits it.

Two practical points must be emphasized. First, and most importantly, **defense counsel must specifically ask prosecutors if account preservation occurred, and if so, when the preservation request was filed.** Counsel should ask this question whenever the government obtained the contents of a client's Internet account. Prosecutors will disclose that a warrant was obtained under 18 U.S.C. § 2703(a) to compel the account contents, and that process is often preceded by preservation. But prosecutors ordinarily will not disclose prior preservation unless specifically asked. This is covered in the article at pages 777-78 and 804.

Second, the primary factual question in this motion is the period of time between preservation under § 2703(f) and the warrant being obtained under § 2703(a). The period is quite long in a typical case, as the statute allows up to 180 days of preservation. But if the period is particularly short or particularly long, counsel should adjust the discussion in Part C accordingly.

It is also worth knowing that in April 2022, the Ninth Circuit initially handed down an opinion in *United States v. Rosenow* that included a brief paragraph rejecting a § 2703(f) challenge. However, upon rehearing, on October 3, 2022, the court amended the opinion to remove that analysis. The final version of *Rosenow* declines to address the merits of the challenge, leaving it an open question.

This is a fourth draft, and I expect to update the draft with additional improvements over time. Please send any comments or suggestions for improvement to orin@berkeley.edu. Also, if you file a motion based on this draft, please consider letting me know about it and how it goes

Thanks, Orin Kerr
U.C. Berkeley School of Law

*The following names and facts, all marked in bold and with brackets, must be filled in throughout the motion:*

- ***[DEFENDANT],*** *your client's last name.*
- ***[E-MAIL ADDRESS OR OTHER ACCOUNT IDENTIFIER],*** *the name of the account that was preserved.*
- ***[PROVIDER],*** *your client's Internet provider that received the preservation request*
- ***[PRESERVATION DATE],*** *the date the government requested preservation*
- ***[WARRANT DATE],*** *the date the warrant was obtained*
- ***[NUMBER OF DAYS],*** *the number of days between [PRESERVATION DATE] and [WARRANT DATE].*

**MOTION TO SUPPRESS CONTENTS OF DEFENDANT'S INTERNET ACCOUNT**

Defendant moves this Court for an order suppressing the entire contents of Defendant's Internet account, **[E-MAIL ADDRESS OR OTHER ACCOUNT IDENTIFIER],** as a fruit of its unlawful suspicionless seizure in violation of the Fourth Amendment.

**INTRODUCTION**

Defendant's private messages in his personal Internet account were seized at the government's direction under the claimed authority of a federal statute, 18 U.S.C. § 2703(f) (hereinafter, "the preservation statute"). The preservation statute provides that, "upon the request of a governmental entity," Internet providers "shall . . . retain[]" files in a user's account "for a period of 90 days," renewable for another 90 days. *Id.*

The government believes that the preservation statute allows the government to order copies made of the contents of any person's Internet account, and to have those contents held for the government for up to 180 days, without any cause whatsoever. Based on this understanding, **[PROVIDER],** acting at the government's agent, seized defendant's private contents and held them on the government's behalf for **[NUMBER OF DAYS]** days.

This long-term, government-directed, suspicionless seizure of Defendant's personal messages cannot be reconciled with the Fourth Amendment. Instead of preservation occurring "pending the issuance of a court order," 18 U.S.C. § 2703(f)(1), as the Fourth Amendment and the plain text of the statute require, the government used the preservation statute to gain control of Defendant's account just in case probable cause eventually developed. The government ordered the seizure of the account without probable cause or even reasonable suspicion. Indeed, the government did not obtain a warrant until **[WARRANT DATE],** fully **[NUMBER OF DAYS]** days after the warrantless seizure occurred on **[PRESERVATION DATE]**.

The Fourth Amendment protects the private e-mails and private messages in a password-protected online account. A government-directed copying and setting aside of a person's private account is a Fourth Amendment seizure. Such a warrantless seizure is permitted under the Fourth Amendment only in very limited circumstances, generally based on probable cause and permitted only for a brief period of time. Because the warrantless seizure in this case occurred without any justification and for an extended period, the fruits of that seizure—the contents of the preserved account—must be suppressed.

## STATUTORY AND FACTUAL BACKGROUND

The Stored Communications Act, 18 U.S.C. §§ 2701-11, is a federal statute that regulates government access to the private records of Internet users. Internet providers such as **[PROVIDER]** hold their users' records on their computer network servers. When criminal investigators seek copies of records from the accounts of criminal suspects, investigators obtain the records directly from the Internet providers. The Stored Communications Act establishes the responsibilities and duties of both the government and Internet providers when the government

seeks user information. *See generally* 2 WAYNE LAFAVE, ET AL., CRIMINAL PROCEDURE § 4.8 (4th ed. 2015) (presenting overview of the statute).

This case involves the Stored Communications Act's preservation statute found at 18 U.S.C. § 2703(f). The statute provides:

> (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.

The preservation statute was enacted to ensure government access to user records that might otherwise be deleted before the government obtained legal process. Because obtaining legal process can be time-consuming, the preservation statute "permits the government to direct providers to 'freeze" stored records and communications" of suspects pending the issuance of a warrant or other court order. U.S. DEP'T OF JUST., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 139 (2009).

The key question is when the preservation statute can be used. The government and major Internet providers interpret 18 U.S.C. § 2703(f) to permit unlimited preservation of Internet accounts. *See* Orin S. Kerr, *The Fourth Amendment Limits of Internet Content Preservation*, 65 St. Louis U. L.J. 753, 766-78 (2021) (summarizing government and provider practices) (hereinafter Kerr, *Internet Content Preservation*). As the government interprets the law, the statute allows any government agent, at any time, to order any provider to make and set a side a copy of every file, of any Internet account, without any suspicion whatsoever. *See id.* The government calls this process "preservation," but it is really just suspicionless seizing. Acting on the government's instruction, and as the government's agents, Internet providers make

complete copies of target accounts and save them exclusively for later government use. *See id.* at 784-85.

Based on the belief that the § 2703(f) permits such mass-scale seizures without cause, the federal government and state governments order the preservation of hundreds of thousands of Internet accounts every year. *See id.* at 767-69. This dragnet surveillance practice has gone unchallenged for many years. *See id.* at 755-56. Major Internet providers and the government work together to make this process both automatic and largely secret. *See id.* at 775-78. When a government agent makes a § 2703(f) request, providers will copy and preserve the account contents without question. *See id.* at 772. In the ordinary case, this process is hidden from users. Internet providers do not tell their customers that preservation occurred. And the government ordinarily does not disclose preservation. *See id.* at 775-78.

This case presents a rare constitutional challenge to § 2703(f) preservation because it is a rare case when the fact of preservation was disclosed. On **[PRESERVATION DATE]**, the government submitted a § 2703(f) request to **[PROVIDER]** directing the preservation of Defendant's account, **[E-MAIL ADDRESS OR OTHER ACCOUNT IDENTIFIER]**. In response to that request, **[PROVIDER]** made a copy of Defendant's account. **[PROVIDER]** then set aside the copy and held it for the government.

The account was held for the government until **[WARRANT DATE]**. On that date, **[NUMBER OF DAYS]** days after the preservation had occurred, the government obtained a warrant to justify the account's seizure and subsequent search. When the government submitted the warrant to **[PROVIDER]**, **[PROVIDER]** then complied with the warrant by sending the government the copy of the preserved account that had been created on **[PRESERVATION**

**DATE]**. Defendant now seeks the suppression of the preserved account contents as the product of an unlawful seizure.

## LEGAL ARGUMENT

The warrantless preservation of Defendant's Internet account violated his Fourth Amendment rights. The preservation was government action because it required **[PROVIDER]** to act on the government's behalf. Preservation triggered a Fourth Amendment seizure because it eliminated **[DEFENDANT]**'s exclusive control of his account. It was an unreasonable seizure because it was not based on probable cause or even reasonable suspicion and was not followed promptly by a warrant. Further, the Terms of Service governing **[PROVIDER]** accounts did not eliminate **[DEFENDANT]**'s Fourth Amendment rights. The contents of the account must be suppressed because they are fruits of the unconstitutional preservation and the good-faith exception does not apply. The analysis below addresses each point in turn.

### A. THE PRESERVATION OF DEFENDANT'S ACCOUNT WAS FOURTH AMENDMENT STATE ACTION.

**[PROVIDER]'**s act of preserving **[DEFENDANT]**'s account pursuant to 18 U.S.C. § 2703(f) was government-directed action regulated by the Fourth Amendment. The Fourth Amendment applies to acts of private individuals acting as "instrument[s] or agent[s]" of the Government. *Coolidge v. New Hampshire*, 403 U.S. 443, 487 (1971). A private party acts as a government agent when the government "compelled a private party to perform a search" or the private party otherwise acted pursuant to the "encouragement, endorsement, and participation" of the government. *Skinner v. Railway Labor Executives' Assn.*, 489 U.S. 602, 613–614 (1989).

That test is satisfied here. Section 2703(f) states that "upon the request of a governmental entity," the provider "*shall take all necessary steps* to preserve records and other evidence" in its possession, and that the records "*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." 18 U.S.C. § 2703(f) (emphasis added). By triggering the preservation statute, the government directed what **[PROVIDER]** must do. In response, **[PROVIDER]** fulfilled the government's wishes on the government's behalf. This mandate satisfies the test for state action. *See Skinner*, 489 U.S. at 613 (noting that "compell[ing] a private party to perform a search" makes that private party a Fourth Amendment state actor).

The preservation in this case is Fourth Amendment government action even if compliance with § 2703(f) is considered voluntary instead of a mandatory obligation. In *Commonwealth v. Gumkowki*, 167 N.E.3d 803 (Mass. 2021), a state trooper asked the cellular and Internet service provider Sprint to voluntarily disclose a suspect's cell-site location records without a warrant. Sprint agreed. The Court ruled that Sprint's voluntary disclosure constituted Fourth Amendment state action: When "law enforcement instigates the search by contacting the cell phone company to request information, there is State action. That Sprint could have refused to provide records in response to [the state trooper's] request does not change the fact that he instigated the search." *Id.* at 812.

*United States v. Hardin*, 539 F.3d 404 (6th Cir. 2008), confirms the point. In *Hardin*, an apartment manager entered an apartment at the request of the government to see if the defendant was present. The Sixth Circuit ruled that the apartment manager was a Fourth Amendment state actor. *Id.* at 407. This was true, the court ruled, "because the officers urged the apartment manager to investigate and enter the apartment, and the manager, independent of his interaction with the officers, had no reason or duty to enter the apartment." *Id.*

When **[PROVIDER]** complied with the government's directive under the preservation statute, both the government and **[PROVIDER]** believed that **[PROVIDER]**'s compliance with

the government's "request" was mandatory. The statute imposes an obligation: It states what a provider "shall" do when it receives a preservation request. 18 U.S.C. § 2703(f). This is not merely "instigat[ing]" the provider's act under *Gumkowski* and *Hardin*, it is "compell[ing] a private party" to act under *Skinner*. But whether the preservation is construed as ordering or merely instigating the act of preservation, it is state action under the Fourth Amendment.

### B. PRESERVATION OF [DEFENDANT]'S ACCOUNT WAS A FOURTH AMENDMENT SEIZURE.

A Fourth Amendment seizure occurs "when there is some meaningful interference with an individual's possessory interests in that property." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). The classic example of a seizure is physical taking away of property. Being "dispossessed" of your property by government action causes a seizure of it. *Soldal v. Cook County*, 506 U.S. 56, 61 (1992) (towing away a mobile home).

Preservation of **[DEFENDANT]**'s account caused a Fourth Amendment seizure because it dispossessed him of control over the account. Internet providers "execute preservation requests by making a copy of the full contents of the relevant account and storing it separately." Kerr, *Internet Content Preservation*, at 771. Although this process is labeled 'preservation,' it reality it is "a dynamic process of entry, copying, and storage." *Id*. at 782. As Internet providers have themselves explained, this is done by performing a "data pull" of the contents of the account that take a "snapshot" of the account contents. *Id.* (quoting public statements from Twitter and Apple). The copy is then stored outside the user's control so the user cannot alter or delete any files. *Id.* at 784-85.

The government-directed act of creating a government copy of the account, and storing it away for later government access, caused a "meaningful interference" with **[DEFENDANT]**'s "possessory interests in that property" because it denied him control over his private information.

*Jacobsen*, 466 U.S. at 113. "Possession" is defined as the "detention and control. . . of anything which may be the subject of property." BLACK'S LAW DICTIONARY 1047 (5th ed. 1979). Before preservation occurred, **[DEFENDANT]** had control of his account contents. He could view this files, he could alter his files, and he could delete his files as he wished.

Preservation eliminated that control. Preservation ensured that a perfect copy of the account contents was generated and detained outside his control exclusively for the government's future use. This was done for the express purpose, and with the exact effect, that **[DEFENDANT]** could no longer control the contents of his account. Preservation therefore triggered a seizure. *See United States v. Bach*, 310 F.3d 1063, 1067-68 (8th Cir. 2002) (analyzing the copying and review of stored Internet contents held by an Internet provider as a Fourth Amendment "seizure" and a "search" of the contents); *Vaugh v. Baldwin*, 950 F.2d 331, 334 (6th Cir. 1991) (noting that, in the absence of consent, the government had "no right to . . . photocopy" a person's private documents); *United States v. Loera*, 333 F. Supp. 3d 172, 185 (E.D.N.Y. 2018) ("Most courts that have addressed duplication, including digital duplication, have analyzed it as a seizure."); Fed. R. Crim. Pro. 41(e)(2)(B) (equating the seizure of electronically stored information with the copying of the information).[1]

In the data context, of course, the government dispossesses a person of control without physically removing the data. But that makes no legal difference. Copying private files triggers a seizure because the government gains control of the data. The government's gaining control and a user's losing exclusive control causes a seizure even though the user still has access to a prior

[1] The Second Circuit expressly held that copying a file is a seizure in a panel decision that was later vacated on rehearing en banc; the en banc court did not reach the question. *See United States v. Ganias*, 755 F.3d 125, 137 (2d Cir. 2014) (holding that the Government's retention of electronic copies of the defendant's personal computer "deprived him of exclusive control over those files," which was "a meaningful interference with [the defendant's] possessory rights in those files and constituted a seizure within the meaning of the Fourth Amendment."), *vacated by United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016) (en banc).

copy of the data. *See United States v. Jefferson,* 571 F. Supp. 2d 696, 703 (E.D. Va. 2008) (holding that "recording . . . information by photograph or otherwise" is a seizure, "even if the document or disc is not itself seized," because "the Fourth Amendment privacy interest extends not just to the paper on which the information is written or the disc on which it is recorded but also to the information on the paper or disc itself"). The government cannot simply take control of the contents of everyone's private Internet messages, just as long as the government does not (yet) look at the files, entirely at the government's whim. Preservation triggers copying of the account, and that copying is a Fourth Amendment seizure permitted only if it is constitutionally reasonable. *See id.*

It should be especially clear that preservation is a Fourth Amendment "seizure" given how Internet search warrants are executed under the Stored Communications Act as required by the Fourth Amendment. *See Warshak v. United States*, 631 F.3d 266, 274 (6th Cir. 2010) (holding that accessing private emails is a Fourth Amendments search that requires a warrant). When the government serves a warrant on a provider under § 2703(a), the provider will run off a copy of the account and send the copy to the government for its review. The provider conducts the initial "seizure," and the government conducts the subsequent "search." *Cf. Bach*, 310 F.3d at 1067-68. Preservation under § 2703(f) is the "seizure" part of the Stored Communications Act's procedure for obtaining Internet account contents. Preservation does not cause a search to occur, because information is not yet revealed to the government. But the transfer of control of account contents under § 2703(f) is a seizure independently of any subsequent search, and it must be independently justified as reasonable. *See Soldal,* 506 U.S. at 61 (explaining that seizures must be justified under the Fourth Amendment independently of any searches).[2]

[2] A small number of trial courts have reasoned that copying account contents are not seizures in the special context of copying files stored outside the United States. *See, e.g., United States v. Gorshkov*, 2001 WL 1024026, at

### C. [PROVIDER]'S TERMS OF SERVICE DID NOT ELIMINATE [DEFENDANT]'S FOURTH AMENDMENT RIGHTS.

The violation of Defendant's Fourth Amendment rights was not lessened or eliminated by the Terms of Service that apply to **[PROVIDER]**'s accounts. Terms of Service found in contracts of adhesion between Internet providers and their users cannot control users' Fourth Amendment rights.

Some background is in order. Every Internet account is governed by Terms of Service, also known as Terms of Use. Terms of Service are contractual terms, drafted by lawyers for the provider, that govern when Internet users can sue the corporation that provides the service for the service that it provides. As a condition of using the service, every user must agree to the Terms. To ensure users cannot sue providers for complying with law enforcement requests, Terms often state that the provider retains the right to comply with those requests. *See, e.g.*, Meta Terms of Service, *available at* https://mobile.facebook.com/privacy/policy/version/20220104/ (reserving the right to "access, preserve and share your information with . . . law enforcement . . . [i]n response to a legal request").

Whatever legal effect Terms of Service may have, they do not eliminate user Fourth Amendment rights or amount to consent. Terms of Service are private contracts between private Internet companies and private users such as the defendant. Although an access agreement between a private person and *the government* can create consent to a search or seizure, an access agreement between a private person and company such as **[PROVIDER]** cannot.

This point is clearly established by caselaw about rental car contracts and apartment leases. For example, in *Byrd v. United States*, 138 S.Ct. 1518 (2018), the Supreme Court held

*3 (W.D. Wash. May 23, 2001) (copying from a server in Russia); *In re Search Warrant To Google, Inc.*, 2017 WL 2985391, at *11 (D.N.J. 2017) (copying accounts from servers outside the United States as part of the execution of a cloud warrant). This case does not raise the unique international concerns that underly those decisions.

that being an unauthorized driver of a rental car in violation of the contract does not eliminate a reasonable expectation of privacy in the car. *See id.* at 1529 ("As anyone who has rented a car knows, car-rental agreements are filled with long lists of restrictions. . . .. Few would contend that violating provisions like these has anything to do with a driver's reasonable expectation of privacy in the rental car—as even the Government agrees.") Private contracts such as rental car agreements are about "risk allocation" between companies and customers, and they have "little to do with whether one would have a reasonable expectation of privacy" in the item used. *Id.*

The same is true with apartment leases. In *United States v. Washington*, 573 F.3d 279 (6th Cir. 2009), the government argued that the defendant had no reasonable expectation of privacy in an apartment because his presence violated the apartment's lease. The Sixth Circuit flatly rejected the claim because "the very premise of the government's argument is flawed." *Id*. at 284. Merely violating the contract could not eliminate privacy rights, the court reasoned, as such a rule would have "the intolerable implications" that a person's rights could be easly relinquishied by a common contractual breach. *Id*. at 284. "[W]e reject the notion that the Constitution ceases to apply in these circumstances." *Id.* at 285. *See also State v. Jacques*, 210 A.3d 533 (Conn. 2019) (citing other cases).

What was true for rental car contracts in *Byrd*, and apartment leases in *Washington*, is equally true for Terms of Service in this case. Terms of Service for Internet accounts are written by corporate lawyers to allocate corporate risk. Terms of Service ensure that a company cannot be sued for violating the service's privacy policy when taking steps the company is legally obligated to take or may want to take for legitimate business reasons. *See* Judith A. Powell & Lauren Sullins Ralls, *Best Practices for Internet Marketing and Advertising*, 29 Franchise L.J. 231, 235 (2010) (advising website operators on considerations for crafting Terms of Service).

To limit corporate liability, Terms of Service are written to limit user permissions while granting providers broad rights. *See, e.g., United States v. Nosal*, 676 F.3d 854, 860–63 (9th Cir. 2012) (providing examples). Such form language designed to minimize corporate risk did not narrow or eliminate Fourth Amendment rights in *Byrd* or *Washington* and cannot do so here.

It is true that some courts have suggested or held that Terms of Service can control Fourth Amendment rights. Courts have divided on the question. *See* Orin S. Kerr, *Terms of Service and Fourth Amendment Rights*, U. Pa. L. Rev. at 7-16 (forthcoming 2023), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4342122. But as Professor Kerr explains, the more persuasive view is that private contracts such as Terms of Service cannot have that effect. They cannot lessen a reasonable expectation of privacy, and they cannot generate consent. *See id*. at 16-37. The caselaw to the contrary has wrongly relied on precedent about agreements with the government, such as those in the government workplace. *See id.* at 24-38. But that caselaw cannot apply to a contract with a private company such as **[PROVIDER]**.

Finally, even if Terms of Service could eliminate Fourth Amendment rights in theory, they cannot do so in practice because the formal act of clicking on a box to agree to Terms of Service cannot be construed as granting consent under *Florida v. Jimeno*, 500 U.S. 248 (1991). *Jimeno* held that the scope of consent is determined by asking "what would the typical reasonable person have understood by the exchange" purporting to grant consent. *Id.* at 251. As applied to Internet accounts, the question is whether a reasonable person observing a user's formal agreement to Terms of Service would understand the user to have actually consented to its specific language.

The answer to that question is "no." A reasonable person would not understand the formality of agreeing to Terms of Service as signifying actual agreement to its terms for a simple

reason: Internet users almost never read Terms of Service. *See* Caroline Cakebread, *You're Not Alone, No One Reads Terms of Service Agreements*, Business Insider, November 17, 2017, https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11 (discussing studies).

For example, in one study, academic researchers created a fake social media site called NameDrop. The Term of Use required "all users" of NameDrop "to immediately assign their first-born child to NameDrop, Inc." Jonathan A. Obar &Anne Oeldorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*, Information, Communication & Society 12 (2018).[3] Only about 2% of site users objected to the term, as 74% of users did not view the Terms of Service and most who viewed them scrolled through the legalese too quickly to understand them. *See id*. at 2.

Obviously, a "typical reasonable person" would not interpret a user's clicking on a box to express agreement with NameDrop's Terms of Service as actually consenting to give their first-born child away. *Jimeno*, 500 U.S. at 251. Rather, a reasonable person would interpret clicking on the box as just agreeing to use the site without concern for what the Terms say. *See* Obar & Oeldorf-Hirsch, *supra*. The same is true for **[DEFENDANT]**'s act of clicking on the box to use a **[PROVIDER]** account. Whatever legal effect the Terms of Service may have in other contexts, clicking on a box to use the service cannot eliminate **[DEFENDANT]**'s Fourth Amendment rights and does not establish consent.

### D. THE GOVERNMENT CANNOT SATISFY ITS BURDEN OF ESTABLISHING THAT THE WARRANTLESS SEIZURE OF THE ACCOUNT WAS REASONABLE.

[3] This paper is available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757465.

"If the defendant meets his burden of establishing a warrantless seizure, the burden then shifts. The Government must establish the warrantless seizure was reasonable." *United States v. Shrum*, 908 F.3d 1219, 1229 (10th Cir. 2018). The government cannot meet that burden. The contents of **[DEFENDANT]**'s Internet account were seized on **[PRESERVATION DATE].** Those contents were held without a warrant until **[WARRANT DATE]**, when probable cause was finally asserted and a warrant was served to permit the disclosure of the account contents to the government. This government-directed suspicionless seizure, occurring for **[NUMBER OF DAYS]** days, cannot be upheld as reasonable under the Fourth Amendment.

The government might seek to justify the seizure as reasonable on two grounds. First, it might claim that the seizure was justified by the existence of probable cause. Second, it might claim that the seizure was permitted by general reasonableness principles without probable cause. As the discussion below shows, neither argument is persuasive.

***(1) The Seizure Cannot Be Justified Based on Probable Cause.***

Probable cause at the inception of a seizure permits the government to temporarily detain property pending the issuance of a warrant. *See United States v. Place*, 462 U.S. 696, 701 (1983) ("Where law enforcement authorities have probable cause to believe that a container holds contraband or evidence of a crime, but have not secured a warrant, the Court has interpreted the Amendment to permit seizure of the property, pending issuance of a warrant to examine its contents, if the exigencies of the circumstances demand it or some other recognized exception to the warrant requirement is present."). This authority allows the government to seize property based on probable cause so long as agents proceed to work diligently to obtain a warrant that permits the property's long-term seizure and subsequent search. *See id.* The preservation statute expressly contemplates this temporary and limited role, as it limits preservation to circumstances

"pending the issuance" of a warrant (for contents) or other legal process (for non-content records). 18 U.S.C. § 2703(f)(1).

The seizure of **[DEFENDANT]**'s Internet account cannot be justified on this basis for two reasons. First, the seizure of the account was not based on probable cause. The temporary warrantless seizure of property must be justified "at its inception." *United States v. Sharpe*, 470 U.S. 675, 482 (1985). But the government did not have the probable cause needed to justify the preservation at its inception. As Professor Kerr has explained, "[p]reservation letters are typically submitted early in an investigation just in case probable cause eventually emerges." Kerr, *Internet Content Preservation*, at 766. When investigators learn a suspect has an online account, they will submit a preservation request to seize the account. *See id.* A common government strategy is to seek "unlimited preservation, just in case probable cause might emerge," *id*. at 757, in order to "ensure that every record in existence at the outset is available if probable cause later develops." *Id.* at 757. About half the time, governments do not follow up with any legal process at all, much less with a warrant needed to compel the contents of an account. *See id.* at 770.

Although this is a case when the government did follow up—the government eventually obtained a warrant under 18 U.S.C. § 2703(a)—a warrantless seizure must be justified "at its inception." *Sharpe*, 470 U.S. at 682. On **[PRESERVATION DATE]**, the date the government directed the preservation of the account, the government lacked probable cause to believe the account contained evidence. The government bears the burden of establishing sufficient cause at the time of the seizure, *see id.* at 709, and it has provided no basis to conclude it can satisfy that burden.

The warrantless seizure was unreasonable for a second reason. Even assuming the government can establish probable cause at the time of preservation, the seizure was

unreasonable because the government waited too long to obtain a warrant. When the government seizes property without a warrant based on probable cause, "the Fourth Amendment requires that they act *with diligence* to apply for a search warrant." *United States v. Smith*, 967 F.3d 198, 202 (2d Cir. 2020) (emphasis added). When the government fails to seek a warrant expeditiously, the warrantless seizure violates the Fourth Amendment even if a warrant is later obtained. *See id.*

*United States v. Mitchell*, 565 F.3d 1347 (11th Cir. 2009), provides a useful reference point. In *Mitchell*, the Eleventh Circuit ordered the suppression of a computer hard drive because investigators allowed 21 days to elapse after seizing the hard drive before they obtained a warrant. The government had validly seized the computer based on exigent circumstances, as there was probable cause to believe it contained child pornography. But the case agent then left town for two weeks of training, and he did not obtain a warrant until he returned and the computer had been seized for 21 days. *See id.* at 1349-50. In ordering suppression of the hard drive and its contents, the Eleventh Circuit held that the 21-day period was unreasonable in the absence of "compelling justification for the delay." *Id.* at 1351. The government's failure to expeditiously apply for a warrant was fatal: "No effort was made to obtain a warrant within a reasonable time because law enforcement officers simply believed that there was no rush." *Id.* at 1353.

*Mitchell* supports suppression in this case. As in *Mitchell*, "[n]o effort was made to obtain a warrant within a reasonable time because law enforcement officers simply believed that there was no rush." *Id.* After preserving on **[PRESERVATION DATE]**, the government waited **[NUMBER OF DAYS]** days until it finally obtained a warrant on **[WARRANT DATE]**. If the 21-day delay between the initial seizure and the warrant in *Mitchell* was too long, surely the **[NUMBER OF DAYS]**-day delay in this case was too long. *See also Smith*, 967 F.3d at 211

(ruling that the Fourth Amendment was violated by a one-month delay after computer seizure before obtaining a warrant).

***(2) The Seizure Cannot Be Justified By General Reasonableness Principles.***

The Government may also try to meet its burden of justifying the seizure of Defendant's account on general reasonableness grounds in the absence of probable cause. Defendant speculates that the Government might try to rely on three distinct lines of cases: (a) the investigative detention principles of *Terry v. Ohio*, 368 U.S. 1 (1968); (b) the "special needs" exception; and (c) the rules for detention during the execution of search warrants. None of these arguments holds water for reasons explained below.

(a) Investigative Detention Doctrine Cannot Justify The Preservation. First, the preservation seizure cannot be justified by the investigative detention principles of *Terry.* It is true that *Terry*'s stop-and-frisk framework can permit a very brief investigative detention of property based only on reasonable suspicion. *See United States v. Place,* 462 U.S. 696, 707 (1983) (allowing the warrantless seizure of luggage based on reasonable suspicion that it contained narcotics). This doctrine has allowed the brief detention of postal mail in transit so drug-sniffing dogs can sniff them for drugs. *See, e.g., United States v. LaFrance*, 879 F.2d 1, 10 (1st Cir. 1989) (allowing detention of FedEx package for 135 minutes based on reasonable suspicion).

But that rule cannot justify the seizure here. A *Terry*-stop detention must be brief. The government can detain property based on reasonable suspicion only to "*quickly* confirm or dispel the authorities' suspicion." *Place*, 462 U.S. at 702 (emphasis added). The seizure can last only as long as the "the police diligently pursued a means of investigation that was likely to confirm or dispel their suspicions *quickly*." *Sharpe*, 470 U.S. at 686 (emphasis added). In *Sharpe*, for

example, the Supreme Court ruled that a 90-minute detention of luggage based only on reasonable suspicion was excessive: "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.

Such a limited detention authority cannot justify the seizure of **[DEFENDANT]**'s account for the **[NUMBER OF DAYS]** days that elapsed after the account was preserved before the government obtained a warrant. That period was far too long. Further, even if *Terry* and *Place* can permit a seizure that long in theory, it could not do so here because the government did not have the required reasonable suspicion at the inception of the seizure that the seized account contained evidence.

*(b) The "Special Needs" Doctrine Cannot Justify the Preservation.* The seizure also cannot be justified under the "special needs" doctrine. The special needs doctrine can permit suspicionless searches and seizures "where the program was designed to serve special needs, beyond the normal need for law enforcement." *City of Indianapolis v. Edmond*, 531 U.S. 32, 37 (2000). For example, the Court has allowed some kinds of drunk-driving checkpoints when has been shown to advance a public interest in safety. *See Michigan Dept. of State Police v. Sitz*, 496 U.S. 444, 455 (1990).

The special needs doctrine does not justify preservation of **[DEFENDANT]**'s account for two reasons. First, the preservation was not conducted for a special need beyond the normal need for law enforcement. As the United States Department of Justice itself has emphasized, the purpose of preservation under § 2703(f) is to help criminal investigators with their criminal investigations: Preservation is designed "to minimize the risk" that "evidence may be destroyed or lost before law enforcement can obtain the appropriate legal order compelling disclosure."

U.S. DEP'T OF JUST., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 139 (2009).

That is not a special need. Instead, it is a classic law enforcement interest in seizing evidence of crime to prevent its destruction. *See Edmond*, 531 U.S. at 48 (concluding that narcotics checkpoints cannot be justified under the special needs exception because their "primary purpose . . . is ultimately indistinguishable from the general interest in crime control"); *Ferguson v. City of Charleston*, 532 U.S. 67, 83-84 (2001) (ruling that drug testing program was not covered by the special needs doctrine because "the immediate objective of the searches was to generate evidence for law enforcement purposes").

Second, even if preservation were somehow deemed a special need (which it clearly is not), it cannot satisfy the reasonableness requirement imposed on special needs seizures. *See, e.g.*, *Illinois v. Lidster*, 540 U.S. 419, 427-78 (2004) (considering whether a special-needs seizure was constitutionally reasonable by weighing the government interests advanced by the seizure and the citizen interests infringed by it). The preservation authority the government claims to have is astonishing. It is the power to seize any person's online account, at any time, for any reason—or even for no reason at all. In the government's view, anyone's online account—even *everyone*'s online account, as the government can preserve multiple accounts at once—can be seized entirely at the government's discretion. The limitless discretion the government claims cannot satisfy any reasonableness test.

*Delaware v. Prouse*, 440 U. S. 648 (1979), is instructive. In *Prouse*, the Supreme Court invalidated a program of suspicionless traffic stops to determine if drivers had a valid license and registration. *See id.* at 663. The government claimed that the discretionary stops were reasonable under the special needs doctrine because checking for license and registration advanced the

public interest in traffic safety. *See id.* at 658. Although the Court agreed that traffic safety was a special need, *see id.* at 658-59, the Court ruled that such seizures without reasonable suspicion were unreasonable. *See id.* at 659-63. "The marginal contribution to roadway safety possibly resulting from a system of spot checks cannot justify subjecting every occupant of every vehicle on the roads to a seizure—limited in magnitude compared to other intrusions but nonetheless constitutionally cognizable—at the unbridled discretion of law enforcement officials." *Id.* at 661. This was especially true because "[a]utomobile travel is a basic, pervasive, and often necessary mode of transportation," *id*. at 662, so that the power to stop cars without reasonable suspicion impacted almost everyone: The Fourth Amendment did not permit such an "evil" of "standardless and unconstrained discretion." *Id.* at 661.

The reasoning of *Prouse* is equally applicable to Internet content preservation under 18 U.S.C. § 2703(f). Modern Internet communications services and devices are "such a pervasive and insistent part of daily life" that using them is "indispensable to participation in modern society." *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018). "The marginal contribution" to Internet crime investigations "resulting from a system" of discretionary Internet preservation "cannot justify subjecting every [user] of every [service on the Internet] to a seizure—limited in magnitude compared to other intrusions but nonetheless constitutionally cognizable—at the unbridled discretion of law enforcement officials." *Prouse*, 440 U.S. at 661.

*(C) Rules for Detention During the Execution of a Warrant Cannot Justify Preservation*. The government might also try to justify the suspicionless seizure of **[DEFENDANT]**'s account under the detention principles of *Michigan v. Summers*, 452 U.S. 692 (1981). *Summers* held that officers executing a search warrant can detain persons on the premises without additional

particularized suspicion. *See id.* at 701. This is justified, the Court reasoned, by the government's interest in preventing flight as well as protecting officer safety. *See id.* at 701-05.

*Summers* cannot justify a preservation seizure because its reasoning was expressly dependent on the government having already obtained a warrant. "Of prime importance in assessing the intrusion," the Court explained, "is the fact that the police had obtained a warrant to search respondent's house for contraband." *Id*. at 701. Detention of those on the premises was reasonable without additional cause because "[a] neutral and detached magistrate had found probable cause to believe that the law was being violated in that house and had authorized a substantial invasion of the privacy of the persons who resided there." *Id.* The warrant had to come first, and obtaining it then justified the lesser intrusion of brief detention. Establishing probable cause "sufficient to persuade a judicial officer that an invasion of the citizen's privacy is justified" made it "constitutionally reasonable to require that citizen to remain while officers of the law execute a valid warrant to search his home." *Id.* at 704-05.

The opposite happened here. The government ordered preservation just in case probable cause might eventually emerge. A warrant was obtained, but not until **[NUMBER OF DAYS]** days later. This case involves seizing just in case a warrant might someday be legally obtained, not seizing as part of the execution of an existing warrant. *Summers* does not apply.

### E. THE ENTIRE CONTENTS OF [DEFENDANT]'S ACCOUNT MUST BE SUPPRESSED AS FRUITS OF THE POISONOUS TREE.

Defendant believes that the preserved copy of his Internet account was turned over to the Government when it served a warrant on **[PROVIDER]** on **[WARRANT DATE]**. Because the Government only had access to that preserved copy as a result of its prior constitutional violation, the entire contents of Defendant's account must be suppressed as fruits of the poisonous tree under *Wong Sun v. United States*, 371 U.S. 471 (1963).

Suppression is appropriate when it "results in appreciable deterrence." *Herring v. United States*, 555 U.S. 135, 141 (2009). That is the case here. Suppression is needed to deter massive-scale and ongoing violations of the Fourth Amendment. Every year, hundreds of thousands of Internet accounts are preserved based on the erroneous assumption that 18 U.S.C. § 2703(f) permits unlimited and suspicionless preservation. *See* Kerr, *Internet Content Preservation*, at 755. Preservation occurs almost entirely in secret, and therefore has gone unchallenged, because governments and Internet providers do not notify their users that preservation has occurred. *See id.* at 771, 775-78. Preservation has occurred on a massive scale nationwide because it has been treated—wrongly, and in the absence of caselaw—as a constitution-free process.

Suppression of the evidence in this case would have a powerful effect "in deterring Fourth Amendment violations in the future." *Herring*, 555 U.S. at 141. A single court ruling could alter practices nationwide. At present, "preservation under § 2703(f) occurs on a wide scale with little scrutiny because law enforcement and providers consider it a privacy non-event." Kerr, *Internet Content Preservation*, at 756. Many if not most preservations that occur today likely violate the Fourth Amendment. A decision from this court suppressing the evidence would be read and digested by both government lawyers nationwide and lawyers at the major Internet providers. A suppression order in this case would force the government to bring its preservation practices into constitutional bounds. It would both limit when investigators seek preservation and trigger provider scrutiny of preservation requests.

A suppression order would have an indirect effect, as well. By identifying constitutional limits on preservation, this court's ruling would encourage providers to disclose preservation to their users, and force governments to disclose preservation to defendants, so that other individuals could more readily litigate potential violations of their Fourth Amendment rights. It

is rare that a single court ruling could have such a nationwide impact. But this is such a case. Under Supreme Court precedent, that deterrent effect justifies suppression. *See Herring*, 555 U.S. at 700.

Finally, the good-faith exception of *Illinois v. Krull*, 480 U.S. 340 (1987), poses no barrier to suppression. *Krull* held that the exclusionary rule does not apply "when officers act in objectively reasonable reliance upon a statute authorizing warrantless administrative searches, but where the statute is ultimately found to violate the Fourth Amendment." *Id.* at 342. Officers are entitled to rely on legislative judgments that searches are constitutional, *Krull* reasoned, at least when those legislative judgments are reasonable. *See id.* at 349-50.

*Krull* does not apply because the mistake here belongs to law enforcement instead of Congress. When Congress enacted 18 U.S.C. § 2703(f), it did not make any legislative judgments about what law enforcement seizures are permitted or when they are constitutional. The preservation statute is not directed to governments at all. The Fourth Amendment governs when a preservation request can be made, and the preservation statute does not say otherwise. The preservation statute merely specifies what Internet providers such as **[PROVIDER]** must do when a government preservation request is made. "[U]pon the request of a governmental entity," the statute says, "[a] provider . . . shall take all necessary steps to preserve records and other evidence in its possession" 18 U.S.C. § 2703(f)(1).

It may be that investigators erroneously believed that § 2703(f) authorizes unlimited preservation. But, if so, that is a law enforcement mistake that falls outside *Krull*. Because there is no legislative error to defer to, the government cannot rely on *Krull* to avoid suppression. *See United States v. Wallace*, 885 F.3d 806, 811 n.3 (5th Cir. 2018) (noting, in a Fourth Amendment challenge brought to surveillance claimed to be authorized by the Stored Communications Act,

that "[t]he holding of *Krull* does not extend to scenarios in which an officer erroneously, but in good faith, believes he is acting within the scope of a statute"); *People v. Madison*, 520 N.E.2d 374, 380 (Ill. 1988) (ruling that *Krull* cannot apply where a "police officer reasonably relies on his own interpretation of a valid statute in conducting a search and seizure" but courts later reject that interpretation).

Put another way, *Krull* only applies when a legislature enacts an unconstitutional law that law enforcement reasonably followed. Here, however, Congress enacted a perfectly constitutional law. Law enforcement's unconstitutional application of the preservation statute is law enforcement's fault, not the fault of Congress. The exclusionary rule should apply.

## CONCLUSION

For the foregoing reasons, the Defendant respectfully requests that this court suppress all evidence obtained as a result of the unlawful seizure of Defendant's account. In the alternative, this Court should order an evidentiary hearing to determine whether to grant this Motion to Suppress.

Respectfully submitted.