

No. 26-4303

**IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT**

IN RE: APPLICATION OF THE UNITED STATES OF
AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)

On Appeal from the United States District Court
for the Eastern District of Virginia, No. 4:25-dm-1 (4:25-ec-25) (Hanes, J.)

**BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION AND
AMERICAN CIVIL LIBERTIES UNION OF VIRGINIA IN SUPPORT OF
APPELLANT**

Eden B. Heilman
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
OF VIRGINIA
P.O. Box 26464
Richmond, VA 23261
(804) 523-2152
eheilman@acluva.org

Nathan Freed Wessler
Laura Moraff
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500
nwessler@aclu.org

Counsel for Amici Curiae

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

DISCLOSURE STATEMENT

- In civil, agency, bankruptcy, and mandamus cases, a disclosure statement must be filed by **all** parties, with the following exceptions: (1) the United States is not required to file a disclosure statement; (2) an indigent party is not required to file a disclosure statement; and (3) a state or local government is not required to file a disclosure statement in pro se cases. (All parties to the action in the district court are considered parties to a mandamus case.)
- In criminal and post-conviction cases, a corporate defendant must file a disclosure statement.
- In criminal cases, the United States must file a disclosure statement if there was an organizational victim of the alleged criminal activity. (See question 7.)
- Any corporate amicus curiae must file a disclosure statement.
- Counsel has a continuing duty to update the disclosure statement.

No. 26-4303 Caption: In Re: Application of USA for Order Pursuant to 18 U.S.C. § 2703(d)

Pursuant to FRAP 26.1 and Local Rule 26.1,

American Civil Liberties Union and American Civil Liberties Union of Virginia
(name of party/amicus)

who is _____ amici curiae _____, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐ YES ☒ NO
2. Does party/amicus have any parent corporations? ☐ YES ☒ NO
If yes, identify all parent corporations, including all generations of parent corporations:
3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐ YES ☒ NO
If yes, identify all such owners:

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation? ☐ YES ☒ NO
If yes, identify entity and nature of interest:
5. Is party a trade association? (amici curiae do not complete this question) ☐ YES ☐ NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:
6. Does this case arise out of a bankruptcy proceeding? ☐ YES ☒ NO
If yes, the debtor, the trustee, or the appellant (if neither the debtor nor the trustee is a party) must list (1) the members of any creditors' committee, (2) each debtor (if not in the caption), and (3) if a debtor is a corporation, the parent corporation and any publicly held corporation that owns 10% or more of the stock of the debtor.
7. Is this a criminal case in which there was an organizational victim? ☐ YES ☒ NO
If yes, the United States, absent good cause shown, must list (1) each organizational victim of the criminal activity and (2) if an organizational victim is a corporation, the parent corporation and any publicly held corporation that owns 10% or more of the stock of victim, to the extent that information can be obtained through due diligence.

Signature: /s/ Nathan Freed Wessler

Date: August 4, 2026

Counsel for: Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

INTEREST OF AMICI CURIAE1

ARGUMENT1

 I. A D-Order must satisfy the Fourth Amendment’s reasonableness
 requirement.....5

 II. Users’ interests must be considered in determining whether a D-
 Order satisfies the Fourth Amendment’s reasonableness
 requirement.....7

 III.A D-Order is unconstitutionally unreasonable if it is overbroad,
 seeks irrelevant records, or otherwise unduly burdens users’
 privacy interests9

 IV.A D-Order recipient must be able to represent its users’ interests in
 moving to quash the order11

 A. Many users have no choice but to rely on service providers
 to quash unconstitutional or illegal D-Orders12

 B. Providers’ ability to raise their users’ interests in moving to
 quash D-Orders is consistent with the SCA’s text and
 purpose15

CONCLUSION22

CERTIFICATE OF COMPLIANCE23

CERTIFICATE OF SERVICE24

TABLE OF AUTHORITIES

Cases

<i>Carpenter v. United States</i> , 585 U.S. 296 (2018).....	1, 2, 4, 6
<i>Chatrie v. United States</i> , No. 25-112, 2026 WL 1855568 (U.S. June 29, 2026).....	1, 2
<i>Doe v. United States</i> , 253 F.3d 256 (6th Cir. 2001)	6
<i>Donovan v. Lone Steer, Inc.</i> , 464 U.S. 408 (1984).....	6
<i>Enterline v. Pocono Medical Center</i> , 751 F. Supp. 2d 782 (M.D. Pa. 2008).....	17
<i>Hale v. Henkel</i> , 201 U.S. 43 (1906).....	5, 10
<i>In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)</i> , 830 F. Supp. 2d 114 (E.D. Va. 2011)	12
<i>In re Applications of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)</i> , 206 F. Supp. 3d 454 (D.D.C. 2016).....	3, 15
<i>In re Grand Jury Subpoena Issued to Twitter, Inc.</i> , No. 3:17-MC-40-M-BN, 2017 WL 9485553 (N.D. Tex. Nov. 7, 2017).....	17, 18
<i>In re Grand Jury Subpoena: Subpoena Duces Tecum</i> , 829 F.2d 1291 (4th Cir. 1987)	11, 16
<i>In re Sealed Case</i> , 144 F.4th 329 (D.C. Cir. 2025).....	20
<i>In re Subpoena Duces Tecum</i> , 228 F.3d 341 (4th Cir. 2000)	6
<i>In re Verizon Internet Services, Inc.</i> , 257 F. Supp. 2d 244 (D.D.C. 2003).....	17

<i>Leaders of a Beautiful Struggle v. Baltimore Police Department</i> , 2 F.4th 330 (4th Cir. 2021)	1
<i>Maness v. Meyers</i> , 419 U.S. 449 (1975).....	14
<i>McVicker v. King</i> , 266 F.R.D. 92 (W.D. Pa. 2010)	17
<i>Murphy v. Waterfront Commissioner of New York Harbor</i> , 378 U.S. 52 (1964).....	5
<i>Oklahoma Press Publishing Company v. Walling</i> , 327 U.S. 186 (1946).....	6, 10
<i>Olmstead v. United States</i> , 277 U.S. 438 (1928) (Brandeis, J., dissenting).....	5
<i>Reich v. Montana Sulphur & Chemical Company</i> , 32 F.3d 440 (9th Cir. 1994)	7
<i>Riley v. California</i> , 573 U.S. 373 (2014).....	1
<i>Schmidt v. City of Norfolk</i> , No. 26-1227 (4th Cir. July 2023, 2026).....	1
<i>Schwimmer v. United States</i> , 232 F.2d 855 (8th Cir. 1956)	passim
<i>See v. City of Seattle</i> , 387 U.S. 541 (1967).....	10
<i>Silverthorne Lumber Company v. United States</i> , 251 U.S. 385 (1920).....	15
<i>Theofel v. Farey-Jones</i> , 359 F.3d 1066 (9th Cir. 2004)	3
<i>Trawinski v. Doe</i> , No. A-0312-14T1, 2015 WL 3476553 (N.J. Super. Ct. App. Div. June 3, 2015)	17

United States v. Clenney,
631 F.3d 658 (4th Cir. 2011)14

United States v. Councilman,
418 F.3d 67 (1st Cir. 2005)..... 3, 20

United States v. Dauphin Deposit Trust Company,
385 F.2d 129 (3d Cir. 1967)6

United States v. Golden Valley Electrical Association,
689 F.3d 1108 (9th Cir. 2012)7

United States v. Harrington,
388 F.2d 520 (2d Cir. 1968) 7, 8, 10, 11

United States v. Information Associated with Email Account (Warrant),
449 F. Supp. 3d 469 (E.D. Pa. 2020).....20

United States v. Morton Salt Company,
338 U.S. 632 (1950).....5

United States v. Ortiz-Orellana,
90 F.4th 689 (4th Cir. 2024)14

United States v. Theodore,
479 F.2d 749 (4th Cir. 1973) 8, 10, 11

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010)4

United States v. Westinghouse Electric Corporation,
638 F.2d 570 (3d Cir. 1980) 13, 15

Statutes

18 U.S.C. § 2703(a)4

18 U.S.C. § 2703(b)4

18 U.S.C. § 2703(c) 4, 13

18 U.S.C. § 2703(d) 12, 15, 16

18 U.S.C. § 2703(e)14

18 U.S.C. § 2712(a)	14
Communications Assistance for Law Enforcement Act, Pub. L. 103-414, § 207, 108 Stat. 4279 (1994).....	3
Electronic Communications Privacy Act of 1986, Pub. L. 99-508, § 201, 100 Stat. 1848 (1986).....	3

Other Authorities

Brief for <i>Amicus Curiae</i> Google LLC in Support of Neither Party, <i>United States v. Chatrie</i> , No. 25-112, 2026 WL 1855568 (U.S. June 29, 2026).....	21
Brief for Microsoft Corp. as <i>Amicus Curiae</i> in Support of Neither Party, <i>United States v. Chatrie</i> , No. 25-112, 2026 WL 1855568 (U.S. June 29, 2026)	21
Brief for Netchoice as <i>Amicus Curiae</i> Supporting Petitioner, <i>United States v. Chatrie</i> , No. 25-112, 2026 WL 1855568 (U.S. June 29, 2026)	21
Brief of X Corp. as <i>Amicus Curiae</i> in Support of Petitioner, <i>United States v. Chatrie</i> , No. 25-112, 2026 WL 1855568 (U.S. June 29, 2026)	21
Brief of <i>Amici Curiae</i> of Technology Companies in Support of Neither Party, <i>United States v. Chatrie</i> , No. 25-112, 2026 WL 1855568 (U.S. June 29, 2026).....	21
<i>LinkedIn Law Enforcement Data Request Guidelines</i> , LinkedIn	13
David Folkenflik, <i>Justice Dept. Drops ‘New York Times’ Subpoenas Under Pressure from Judge</i> , NPR (July 23, 2026).....	19
Eric Boehm, <i>Goodbye and Good Riddance to Operation Choke Point</i> , Reason (Aug. 18, 2017)	19
H.R. REP. No. 103-827 (1994), <i>as reprinted in</i> 1994 U.S.C.C.A.N. 3489	2, 3, 19
<i>Hearing on Permanent Provisions of the PATRIOT Act before the House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security</i> (2011) (Statement of Todd M. Hinnen, Acting Assistant Attorney General for National Security, Department of Justice)	20, 21

Ingrid Kelley, <i>Online Photo of Student with Gun, Threat Sparks Grosse Pointe Schools Investigation</i> , Fox 2 Detroit (Dec. 8, 2017).....	19
Kristine Parks, <i>British Man Says He Was Arrested After Posting Photos Holding Guns During July 4 Trip to Florida</i> , Fox News (Dec. 4, 2025).....	19
Mark Ellis Harris, <i>A Peek Inside the FBI's Unprecedented January 6 Geofence Dragnet</i> , Wired (Nov. 28, 2022)	19
Michael Williams, <i>ICE Officers Warned a New York Man After He Sent a Critical Email to the Agency's Chief. Now He's Suing</i> , CNN (July 6, 2026)	19
<i>New Deloitte Survey: Increasing Consumer Privacy and Security Concerns in the Generative AI Era</i> , Deloitte (Dec. 2, 2024).....	21
Orin S. Kerr, <i>A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It</i> , 72 Geo. Wash. L. Rev. 1208 (2004)	6
Press Release, ACLU, <i>ACLU Moves to Quash Abusive Subpoena Aimed at Tracking Down Man who Criticized Department of Homeland Security</i> (Feb. 3, 2026).....	19
Press Release, Sen. Ron Wyden, United States Senator for Oregon, <i>Wyden Reveals Which Phone Companies Protect Privacy by Telling Customers About Government Surveillance</i> (May 21, 2025).....	13
<i>Reforming The Electronic Communications Privacy Act: Hearing before the Senate Committee on Judiciary</i> (2015) (statement of Elena Tyrangiel, Principal Deputy Assistant Att'y Gen.).....	4
Ryan Devereaux, <i>A Redditor Criticized ICE. Trump Is Trying to Unmask Them By Dragging the Company to a Secret Grand Jury</i> , The Intercept (Apr. 10, 2026).....	19
S. REP. No. 99-541 (1986), <i>as reprinted in</i> 1986 U.S.C.C.A.N. 3555	3, 16
Staff of House Committee on Oversight and Government Reform, 113th Congress, <i>DOJ's Operation Choke Point Secretly Pressured Banks to Cut Ties with Legal Business</i> (2014)	19

INTEREST OF *AMICI CURIAE*¹

The American Civil Liberties Union (“ACLU”) is a nationwide, non-partisan, non-profit organization that since 1920 has sought to protect the civil liberties of all Americans. The ACLU of Virginia is the Virginia state affiliate of the national ACLU. The ACLU and its affiliates have participated as counsel or *amici* in many cases concerning individuals’ privacy interests in digital data. *See, e.g., Chatrie v. United States*, No. 25-112, 2026 WL 1855568 (U.S. June 29, 2026) (*amicus*); *Carpenter v. United States*, 585 U.S. 296 (2018) (counsel); *Riley v. California*, 573 U.S. 373 (2014) (*amicus*); *Schmidt v. City of Norfolk*, No. 26-1227 (4th Cir. July 2023, 2026) (*amicus*); *Leaders of a Beautiful Struggle v. Balt. Police Dep’t*, 2 F.4th 330 (4th Cir. 2021) (counsel).

ARGUMENT

The use of electronic communications services and remote computing services such as social media networks, email providers, and internet service providers has “become a ‘pervasive and insistent’—even ‘indispensable’—‘part of daily life.’” *Chatrie v. United States*, No. 25-112, 2026 WL 1855568, at *16 (U.S. June 29, 2026) (quoting *Carpenter v. United States*, 585 U.S. 296, 315 (2018)).

¹ Pursuant to Federal Rule of Appellate Procedure Rule 29(a)(4)(e), counsel for *amici* certify that no party’s counsel authored this brief in whole or in part. No person other than *amici*, their members, or their counsel contributed money that was intended to fund the preparing or submitting of this brief. All parties have consented to the filing of this brief.

Americans rely on these services every day to communicate with family, friends, and strangers about everything from life updates to employment opportunities to politics, religion, and work.

For more than three decades, “[b]usiness, nonprofit organizations and political groups [have] conduct[ed] their work over the Internet,” and “[i]ndividuals [have] maintain[ed] a wide range of relationships on-line.” H.R. REP. No. 103-827, at 17 (1994), *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3497 (discussing the 1994 amendments to the Electronic Communications Privacy Act). The data that service providers retain thus “reveals a great deal about [individuals’] private lives, all of it compiled in one place.” *Id.* These databases are surveillance gold mines that “run[] against everyone.” *Carpenter*, 585 U.S. at 312.

The information in a user’s online account—such as their LinkedIn account—is “information that a user reasonably understands as his own.” *See Chatrie*, 2026 WL 1855568, at *15 (referring to location history in a Google account). Although the information is stored on the company’s servers, the “exposure of that information to [the company] is merely what happens when a user avails himself of one of the services” on the web. *Id.*

The Stored Communications Act (“SCA”) “reflects Congress’s judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility.” *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072

(9th Cir. 2004). After a Privacy and Technology Task Force “questioned” whether the SCA, in its original form, provided adequate restrictions on government access to private records, H.R. REP. No. 103-827, at 12, the statute was amended “to protect privacy in the face of increasingly powerful and personally revealing technologies.” *Id.* at 13. The amendments served “to guard against ‘fishing expeditions’ by law enforcement.”² *In re Applications of the U.S. for an Ord. Pursuant to 18 U.S.C. § 2703(d)*, 206 F. Supp. 3d 454, 456 (D.D.C. 2016) (quoting H.R. REP. No. 103-827, at 31–32). The Act is designed to “halt . . . potential intrusions on individual privacy,” *United States v. Councilman*, 418 F.3d 67, 80 (1st Cir. 2005), and to “ensure the continued vitality of the [F]ourth [A]mendment,” S. REP. No. 99-541, at 5 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.

The SCA, 18 U.S.C. § 2703, sets out three types of legal process that the government may use to seek user or customer records from a provider of electronic communications services or remote computing services. An administrative or grand jury subpoena may be issued for certain types of basic subscriber records. 18 U.S.C.

² The 1994 amendments, enacted as part of the Communications Assistance for Law Enforcement Act (“CALEA”), strengthened protections for the kinds of records at issue in this case, including by requiring government entities to obtain at least a D-Order (rather than using an administrative subpoena) and raising the threshold for issuance of a D-Order. *Compare* Electronic Communications Privacy Act of 1986, Pub. L. 99-508, § 201, 100 Stat. 1848, 1860 (1986), *with* CALEA, Pub. L. 103-414, § 207, 108 Stat. 4279, 4292 (1994).

§ 2703(c)(2). A warrant is required for contents of electronic communications. *Id.* § 2703(a), (b).³ And either a warrant or an order under Section 2703(d) (hereinafter “D-Order”) may be used to seek “a record or other information pertaining to” a subscriber or user. *Id.* § 2703(c)(2).

Like the other forms of compulsory legal process at issue in the SCA, a D-Order must comply not only with the SCA, but also with the Fourth Amendment. The Fourth Amendment demands that such compulsory process be *reasonable*. The reasonableness of a D-Order turns not simply on the logistical burden on the recipient, but also on the burden on the user whose information is sought. Thus, a user’s privacy interests must be considered in determining whether a D-Order is constitutional. A D-Order that is overbroad, seeks material irrelevant to the investigation, or otherwise unduly burdens users’ privacy interests cannot satisfy the Fourth Amendment and must be quashed. In practice, users in many cases have no

³ Although 18 U.S.C. § 2703(a) requires a warrant only for the contents of communications that have been “in electronic storage in an electronic communications system for one hundred and eighty days or less,” courts have held that under the Fourth Amendment, a warrant is required for communications content regardless of how long it has been in storage, and the federal government has adopted this view. *See United States v. Warshak*, 631 F.3d 266, 286–88 (6th Cir. 2010); *Reforming The Electronic Communications Privacy Act: Hearing before the S. Comm. on Judiciary* 4 (2015) (statement of Elena Tyrangiel, Principal Deputy Assistant Att’y Gen.), <https://perma.cc/DM5Z-8283> (“[T]here is no principled basis to treat email less than 180 days old differently than email more than 180 days old.”). *See also Carpenter*, 585 U.S. at 319.

choice but to rely on providers to protect their interests, and to move to quash any demands for their information that fail to comply with constitutional and statutory requirements. The recipient of a D-Order must therefore be able to invoke its users' privacy interests in challenging the scope and legality of the order.

I. A D-Order must satisfy the Fourth Amendment's reasonableness requirement.

The "right to be let alone," guaranteed by the Fourth Amendment, has been treated as "the most comprehensive of rights and the right most valued by civilized men." *United States v. Morton Salt Co.*, 338 U.S. 632, 651–52 (1950) (quoting *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting)). This right "is not confined literally to searches and seizures as such, but extends as well to the orderly taking under compulsion of process." *Id.* at 651–52 (citation omitted). Indeed, the "substance" of an unreasonable search and seizure "is the compulsory production of private papers, whether under a search warrant or a *subpoena duces tecum*, against which the person, be he individual or corporation, is entitled to protection." *Hale v. Henkel*, 201 U.S. 43, 76 (1906), *overruled on other grounds by* *Murphy v. Waterfront Comm'n of N.Y. Harbor*, 378 U.S. 52 (1964). Thus, "[t]he compelled production of one's private books and papers through a subpoena duces tecum, for use against him in a criminal proceeding, is, of course, as much within the guaranty of the Fourth Amendment against unreasonable searches and seizures

as is a reaching of them by means of a warrant.” *Schwimmer v. United States*, 232 F.2d 855, 860 (8th Cir. 1956) (citation omitted).⁴

As applied to “the production of corporate records and papers in response to a subpoena or order authorized by law and safeguarded by judicial sanction,” the Fourth Amendment requires that “the disclosure sought [] not be unreasonable.” *Okla. Press Publ’g Co. v. Walling*, 327 U.S. 186, 208 (1946); accord *Donovan v. Lone Steer, Inc.*, 464 U.S. 408, 415 (1984); see also *Doe v. United States*, 253 F.3d 256, 264 (6th Cir. 2001) (In contrast to warrants, “subpoenas are analyzed only under the Fourth Amendment’s general reasonableness standard” (citing *In re Subpoena Duces Tecum*, 228 F.3d 341, 347–49 (4th Cir. 2000))); *United States v. Dauphin Deposit Tr. Co.*, 385 F.2d 129, 131 (3d Cir. 1967) (“The requirement that the summons not be indefinite is rooted in the Fourth Amendment protection against unreasonable searches and seizures.”). Even where statutory criteria are satisfied and all procedural requirements have been followed, this “Fourth Amendment

⁴ Although a D-Order is signed by a judge, it is issued on a showing of “‘reasonable grounds’ for believing that the records were ‘relevant and material to an ongoing investigation.’” *Carpenter*, 585 U.S. at 317 (quoting 18 U.S.C. § 2703(d)). “That showing falls well short of the probable cause required for a warrant.” *Id.* The D-Order is then “served like an ordinary subpoena . . . and the [recipient] complies by turning over the information” just as it would in responding to a subpoena. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1219 (2004).

‘reasonableness’ inquiry must also be satisfied.” *United States v. Golden Valley Elec. Ass’n*, 689 F.3d 1108, 1113 (9th Cir. 2012) (quoting *Reich v. Mont. Sulphur & Chem. Co.*, 32 F.3d 440, 444 n. 5 (9th Cir. 1994)).

Because a D-Order compels its recipient to produce private records, it must satisfy the Fourth Amendment’s reasonableness requirement.

II. Users’ interests must be considered in determining whether a D-Order satisfies the Fourth Amendment’s reasonableness requirement.

The Fourth Amendment’s reasonableness inquiry does not turn solely on burdens on the recipient of the compulsory process; it takes into account other affected individuals’ interests as well. Even where the logistical burden on the recipient of the order is “slight” in that the recipient can “segregate the requested records without difficulty,” the requested records still must be “sufficiently relevant to the investigation.” *United States v. Harrington*, 388 F.2d 520, 523 (2d Cir. 1968).

An order compelling disclosure is unreasonable where it “involve[s] an improper intrusion into what is, in relation to the purpose of the investigation, purely private or privileged papers,” regardless of whether the privacy or privilege belongs to the recipient of the order or to another individual whose information is sought. *Schwimmer*, 232 F.2d at 861. “The personal interest cannot be so blithely brushed aside” by orders for the disclosure of information that merely has “some

chance of relevance” or “some possibility of relation” to an investigation.

Harrington, 388 F.2d at 524.

Indeed, “judicial protection against the sweeping or irrelevant order is *particularly* appropriate in matters where the demand for records is directed not to the [individual to whom the records pertain] but to a third-party who may have had some dealing with the person under investigation.” *United States v. Theodore*, 479 F.2d 749, 754 (4th Cir. 1973) (quoting *Harrington*, 388 F.2d at 523).

The Eighth Circuit recognized the importance of a user’s (or customer’s) interest in their information in *Schwimmer*, 232 F.2d 855. There, an attorney moved to quash two grand jury subpoenas that were issued to a third-party storage company requiring the production of records related to one of the attorney’s clients, on the grounds that they were unreasonable under the Fourth Amendment. *Id.* at 858–59. The Court clarified that the “question of whether to issue a subpoena against the owner or against the third party” is “merely one of procedural choice and convenience.” *Id.* at 860. But “[s]ubstantively, each involves, except as to the task of appearing and making delivery, the same aspects of reach, deprivation and seizure-effect against the owner.” *Id.* at 860. In other words, the effect of the subpoena on the individual whose documents are produced is the same whether the documents are produced by the individual or by a third party. The “mere procedural device of compelling a third-party naked possessor to produce and deliver” the

records could not “enable the question of unreasonable search and seizure to be escaped.” *Id.* at 861. This is because “[t]he constitutional safeguard against unreasonable searches and seizures is more than a reach at mechanics in process,” and concerns “reality, not theory, in respect to the whole of what is being done.” *Id.* at 861.

The court held that one of the subpoenas issued to the storage company “would dominantly constitute a general fishing expedition,” and thus “amount[ed] in the situation to an unreasonable search and seizure against [the attorney].” *Id.* at 862.⁵

As *Schwimmer* demonstrates, the “private right affected” is not limited to the recipient of the compulsory process. 232 F.2d at 861. In assessing a D-Order’s reasonableness, courts must consider the burdens on users.

III. A D-Order is unconstitutionally unreasonable if it is overbroad, seeks irrelevant records, or otherwise unduly burdens users’ privacy interests.

The Fourth Amendment’s reasonableness requirement encompasses “relevancy and adequacy or excess in the breadth of the subpoena” or other

⁵ The other subpoena required production of “an attorney’s files of a specific client’s affairs, for a reasonably limited period of time, in a grand jury’s investigation of incidents involved in the attorney’s handling of some of those affairs.” *Schwimmer*, 232 F.2d at 863. The court held that this other subpoena was not “of such unwarranted scope or of such substantial, apparent irrelevancy as to be generally unreasonable.” *Id.*

compulsory process. *See Okla. Press Publ'g Co.*, 327 U.S. at 209. Thus, it has long been “settled” that investigative subpoenas must be “sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome.” *See v. City of Seattle*, 387 U.S. 541, 544 (1967).

The same follows for a D-Order. Like a subpoena, a D-Order should be “deemed unreasonable and unenforceable if it is overbroad and disproportionate to the end sought,” *Theodore*, 479 F.2d at 754 (citing *Harrington*, 388 F.2d at 523), or if it is “so broad in its scope as to go substantially beyond the bounds of apparent relevance in relation to an immediate pursuit and so be unreasonable,” *Schwimmer*, 232 F.2d at 861.

Assessing relevance and overbreadth requires an examination of “the nature, purposes and scope of the inquiry.” *Okla. Press Publ'g Co.*, 327 U.S. at 209. Where a movant seeks to quash a subpoena on relevancy grounds, the question “is whether from what the Government already knows there exists the requisite nexus” between the records and the investigation such that there is a “realistic expectation rather than an idle hope that something may be discovered” in them. *Harrington*, 388 F.2d at 524. Particularly when a demand for records is “sweeping,” there must be “some evidence of their materiality produced, to justify an order for the production of such a mass of papers.” *Hale*, 201 U.S. at 77.

A subpoena will fail to satisfy the Fourth Amendment's reasonableness test if "the thing done or attempted to be done, in the sum of its form, scope, nature, incidents and effect, impresses as being fundamentally unfair or unreasonable in the specific situation, when the immediate end sought is considered against the private right affected." *Schwimmer*, 232 F.2d at 861. And "where it appears that the purpose of the summons is 'a rambling exploration' of a third party's files, it will not be enforced." *Theodore*, 479 F.2d at 754 (quoting *Harrington*, 388 F.2d at 523).

This Court has long insisted "that the guarantees of the [F]irst and [F]ourth [A]mendments not be trampled by overly broad subpoenas." *In re Grand Jury Subpoena: Subpoena Duces Tecum*, 829 F.2d 1291, 1302 n.15 (4th Cir. 1987). In order to maintain those guarantees, courts assessing the reasonableness of a D-Order must carefully analyze the order's relevance to the underlying investigation, the breadth of the information sought, and the privacy invasions of the users whose records would be disclosed.

IV. A D-Order recipient must be able to represent its users' interests in moving to quash the order.

Where the recipient of an unreasonable D-Order moves to quash or modify, that recipient must be able to raise objections based on its users' privacy interests. Users' reliance is fully consistent with the SCA, and this Court should uphold providers' ability to vindicate their users' interests. Otherwise, many users will have no meaningful way to avoid or redress constitutional or statutory violations.

A. Many users have no choice but to rely on service providers to quash unconstitutional or illegal D-Orders.

Because courts have held that the SCA gives only the recipient of the D-Order an express right to challenge it on statutory grounds under Section 2703(d), users must rely on providers to ensure D-Orders do not unreasonably infringe on their interests as protected by the statute.⁶ *See* 18 U.S.C. § 2703(d) (“A court issuing an order pursuant to this section, on a motion made promptly *by the service provider*, may quash or modify such order”) (emphasis added); *In re Application of the U.S. for an Ord. Pursuant to 18 U.S.C. § 2703(d)*, 830 F. Supp. 2d 114, 129 (E.D. Va. 2011) (“[T]he Stored Communications Act does not confer upon [the subject of the investigation] a right to seek non-constitutional review of the [D-Order]” issued to their service provider.). As to constitutional challenges, some courts have held that the ability of the subject of the investigation to bring a motion to quash or vacate a D-Order depends on the type of information the order seeks, and whether the individual has a reasonable expectation of privacy in it. *See In re Application*, 830 F. Supp. 2d at 138–39. If that is right (which *amici* do not concede), then challenge

⁶ A different section of the SCA provides users an express right to move to vacate a D-Order seeking certain contents of communications. 18 U.S.C. § 2704(b). This is unlikely to arise because, since the enactment of the SCA, courts have held that use of a D-Order to seek contents of communications violates the Fourth Amendment, and that a warrant is required instead. *See supra* note 3.

to the D-Order's reasonableness under the Fourth Amendment must be advanced by the service provider's motion.

Regardless of whether the user could in theory challenge a D-Order, where, as here, the government obtains a secrecy order, users will not know that their information has been sought (and likely turned over) at least until the secrecy order expires. And even then, because the government does not provide notice to the user when it seeks non-content records with a D-Order, *see* 18 U.S.C. § 2703(c)(3), the user will only learn of the D-Order if their service provider decides, in its discretion, to tell them. This is true even in cases without secrecy orders; many service providers lack policies of notifying their users of requests for user records,⁷ and even those that have general notice policies are under no legal obligation to provide notice, and so may decline or fail to notify a user in any particular case. This, alone, is reason enough to permit a company to advocate for its users' interests. *See United States v. Westinghouse Elec. Corp.*, 638 F.2d 570, 574 (3d Cir. 1980) (recognizing third-party

⁷ Compare *LinkedIn Law Enforcement Data Request Guidelines*, LinkedIn, <https://perma.cc/UEQ8-HA7A> (noting policy of “notifying members of requests for their data unless prohibited by statute or court order”), with Press Release, Sen. Ron Wyden, United States Senator for Oregon, *Wyden Reveals Which Phone Companies Protect Privacy by Telling Customers About Government Surveillance* (May 21, 2025), <https://perma.cc/W2D7-9LE8> (major cellular service providers do not notify customers of government requests for records).

standing where “the absence of any notice to the employees of the subpoena means that no person other than Westinghouse would be likely to raise the privacy claim.”).

Even if a user eventually learns of the D-Order, by that point, it will be far too late to “unring the bell,” because the user’s information will already have been turned over. *Cf. Maness v. Meyers*, 419 U.S. 449, 460 (1975) (“When a court during trial orders a witness to reveal information . . . [c]ompliance could cause irreparable injury because appellate courts cannot always ‘unring the bell’ once the information has been released.”). And even if the D-Order leads to a criminal prosecution, there may be no remedy available. *See United States v. Clenney*, 631 F.3d 658, 667 (4th Cir. 2011) (finding no suppression remedy for statutory violations under the SCA); *United States v. Ortiz-Orellana*, 90 F.4th 689, 698 (4th Cir. 2024) (holding the good-faith exception to the exclusionary rule applied to cell-site location information obtained with a D-Order), *cert. denied*, 145 S. Ct. 1890 (2025).

Additionally, individuals have little reason to challenge an invalid D-Order after their privacy has already been violated, as litigation is an uphill—and costly—battle. Indeed, service providers are immune from suit if they have disclosed records “in accordance with the terms of” a D-Order, 18 U.S.C. § 2703(e), and an action for damages against the United States can only be maintained if the plaintiff can prove that violation of the statute was “willful,” a difficult evidentiary bar to surmount. 18 U.S.C. § 2712(a). Thus, if a service provider cannot raise violations of its users’

privacy interests prior to compliance with the D-Order, the claim “may be effectively lost.” *Westinghouse Elec. Corp.*, 638 F.2d at 574.

Consequently, users generally have no meaningful option but to rely on providers to represent their privacy interests and move to quash or modify D-Orders that violate statutory or constitutional requirements on their behalf.

B. Providers’ ability to raise their users’ interests in moving to quash D-Orders is consistent with the SCA’s text and purpose.

The SCA permits D-Orders to issue only when “the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the . . . information sought[is] relevant and material to an ongoing criminal investigation.” 18 U.S.C. § 2703(d); *see also In re Applications of the U.S. for an Ord. Pursuant to 18 U.S.C. § 2703(d)*, 206 F. Supp. 3d at 456 (Section 2703(d) requires a “nexus between the investigation and the information” sought.). Where a D-Order has issued in violation of that requirement, it must be quashed. *Cf. Silverthorne Lumber Co. v. United States*, 251 U.S. 385, 392 (1920) (“The essence of a provision forbidding the acquisition of evidence in a certain way is that not merely evidence so acquired shall not be used before the Court but that it shall not be used at all.”).

The Act further provides that a court can quash or modify a D-Order where “the information or records requested are unusually voluminous in nature or

compliance with such order otherwise would cause an undue burden on such provider.” 18 U.S.C. § 2703(d). This provision of standing to service providers “to contest an overly broad order” was intended not only “to protect the service provider from unduly burdensome requirements” but also “to permit an impartial judicial officer to evaluate the appropriateness of the government’s request.” S. REP. NO. 99-541, at 39. In light of the Act’s express requirement that D-Orders seek “relevant and material information,” as well as the Fourth Amendment’s reasonableness requirement, this evaluation of the appropriateness of the order must encompass both the logistical burdens on the recipient of the D-Order and burdens on users’ privacy interests. *Cf. In re Grand Jury Subpoena: Subpoena Duces Tecum*, 829 F.2d at 1300 (“Even when the [F]irst [A]mendment and [F]ourth [A]mendment problems raised by subpoenas duces tecum do not, in and of themselves, rise to the level of constitutional violations, the concerns that underlie those constitutional provisions must enter into the balancing of interests that is required by a motion to quash under Fed.R.Crim.P. 17(c).”).

Additionally, because a service provider’s user base depends on users’ trust and satisfaction, a burden on users—including an undue burden on users’ privacy—amounts to a burden on the provider. This is consistent with “the trend among federal district courts [] to find injury in fact where an organization, like Twitter, whose business provides a valuable medium of expression, is asked [to] betray its

customers' trust by complying with a subpoena." *In re Grand Jury Subpoena Issued to Twitter, Inc.*, No. 3:17-MC-40-M-BN, 2017 WL 9485553, at *8 (N.D. Tex. Nov. 7, 2017), *report and recommendation adopted*, No. 3:17-MC-40-M-BN, 2018 WL 2421867 (N.D. Tex. May 3, 2018); *see also* *McVicker v. King*, 266 F.R.D. 92, 95 (W.D. Pa. 2010) ("The trend among courts which have been presented with this question is to hold that entities such as newspapers, internet service providers, and website hosts may . . . assert the rights of their readers and subscribers."); *Enterline v. Pocono Medical Ctr.*, 751 F. Supp. 2d 782, 786 (M.D. Pa. 2008) (holding that a newspaper had standing to assert the First Amendment rights of commentators on its online forums who "face[d] practical obstacles to asserting their own First Amendment rights"); *Trawinski v. Doe*, No. A-0312-14T1, 2015 WL 3476553, at *5 (N.J. Super. Ct. App. Div. June 3, 2015) (same); *In re Verizon Internet Servs., Inc.*, 257 F. Supp. 2d 244, 258 (D.D.C. 2003) ("The relationship between an Internet service provider and its subscribers is the type of relationship courts have found will ensure that issues will be 'concrete and sharply presented.' Verizon has a vested interest in vigorously protecting its subscribers' First Amendment rights, because a failure to do so could affect Verizon's ability to maintain and broaden its client base."), *rev'd on other grounds sub nom. Recording Indus. Ass'n of Amer., Inc. v. Verizon Internet Servs., Inc.*, 351 F.3d 1229 (D.C. Cir. 2003).

For example, the Northern District of Texas recognized that Twitter had a sufficiently close relationship with its users for third-party standing, because “Twitter and its users reap mutual benefit when Twitter protects its users First Amendment rights.” *In re Grand Jury Subpoena Issued to Twitter, Inc.*, 2017 WL 9485553, at *9. There, Twitter had shown that “enforcement of the Subpoena discourages Twitter’s users . . . from using Twitter’s services and from contributing controversial content,” because “compliance with the Subpoena sends the message to Twitter users worldwide, first, that their anonymous tweets may not stay anonymous and, second, that expressing their unpopular views may subject them to unwanted government investigation.” *Id.* at *8.

Moreover, if logistical burdens on the provider were the only grounds on which a D-Order could be quashed, then the SCA could not serve its purpose of protecting individuals’ privacy in their electronic communications. The government would be able to demand any records it wished—so long as it did so in a way that was logistically easy for the provider. The government could demand *all* of a single user’s account information on the grounds that the user posted a picture of themselves

with a firearm,⁸ criticized a DHS employee,⁹ visited an area near alleged criminal activity,¹⁰ was doing business in a disfavored industry,¹¹ or published a news article addressing national security topics.¹²

That is not the law. The SCA was enacted, and later amended, because Congress recognized that “as the potential intrusiveness of technology increases, it is necessary to ensure that government surveillance authority is clearly defined and appropriately limited.” H.R. REP. No. 103-827, at 17. Congress passed the SCA to address “threats to individual privacy” stemming from “the rise of remote computing

⁸ See Ingrid Kelley, *Online Photo of Student with Gun, Threat Sparks Grosse Pointe Schools Investigation*, Fox 2 Detroit, at 0:22 (Dec. 8, 2017), <https://www.fox2detroit.com/video/419300.amp>; Kristine Parks, *British Man Says He Was Arrested After Posting Photos Holding Guns During July 4 Trip to Florida*, Fox News (Dec. 4, 2025), <https://perma.cc/Y6QL-TRGF>.

⁹ See Press Release, ACLU, *ACLU Moves to Quash Abusive Subpoena Aimed at Tracking Down Man who Criticized Department of Homeland Security* (Feb. 3, 2026), <https://perma.cc/YK75-D2WN>; Michael Williams, *ICE Officers Warned a New York Man After He Sent a Critical Email to the Agency’s Chief. Now He’s Suing*, CNN (July 6, 2026), <https://perma.cc/MWW6-NMNY>; Ryan Devereaux, *A Redditor Criticized ICE. Trump Is Trying to Unmask Them By Dragging the Company to a Secret Grand Jury*, The Intercept (Apr. 10, 2026), <https://perma.cc/ZJ9Y-6V4V>.

¹⁰ See Mark Ellis Harris, *A Peek Inside the FBI’s Unprecedented January 6 Geofence Dragnet*, Wired (Nov. 28, 2022), <https://perma.cc/5BL3-BZGV>.

¹¹ See Staff of H. Comm. on Oversight and Gov’t Reform, 113th Congress, *DOJ’s Operation Choke Point Secretly Pressured Banks to Cut Ties with Legal Business* (2014), <https://perma.cc/GGM7-D52Z>; Eric Boehm, *Goodbye and Good Riddance to Operation Choke Point*, Reason (Aug. 18, 2017), <https://perma.cc/6R3S-3M8J>.

¹² See David Folkenflik, *Justice Dept. Drops ‘New York Times’ Subpoenas Under Pressure from Judge*, NPR (July 23, 2026), <https://perma.cc/KVX9-XUT4>.

operations and large databanks of stored electronic communications.” *Councilman*, 418 F.3d at 80; *see also United States v. Info. Associated with Email Acct. (Warrant)*, 449 F. Supp. 3d 469, 472 (E.D. Pa. 2020) (“The SCA was passed in the wake of congressional concern about protecting individual’s privacy interests in information held online by third parties.”).

The SCA is designed to accomplish its purpose of “protect[ing] the privacy of user data held by electronic communication service providers” by, in part, “regulating government access to that data.” *In re Sealed Case*, 144 F.4th 329, 331 (D.C. Cir. 2025). The SCA can fulfil that purpose only if providers are able to challenge government access when it unduly burdens the privacy of their users.

Many companies have taken this obligation to represent their users’ privacy interests seriously. At a House Judiciary Committee hearing in 2011, a congressman asked a senior Department of Justice representative “why [a service provider] would have an incentive to hire lawyers to protect [its subscribers’ privacy] rights.”¹³ The Department’s representative responded that “Internet service providers take the privacy of their customers and subscribers very seriously and I think are often an

¹³ *Hearing on Permanent Provisions of the PATRIOT Act before the H. Comm. on Judiciary, Subcomm. on Crime, Terrorism, and Homeland Sec.* 65 (2011) (Statement of Todd M. Hinnen, Acting Assistant Att’y Gen. for Nat’l Sec., Dep’t of Just.) <https://perma.cc/GG88-555F>.

effective proxy for defending those rights.”¹⁴ More recently, in landmark Fourth Amendment cases before the Supreme Court, service providers and their trade associations have filed amicus briefs advancing their users’ interests in protecting records from unreasonable searches. *See, e.g.,* Br. of X Corp. as *Amicus Curiae* in Support of Pet’r, *Chatrue*, 2026 WL 1855568; Br. for *Amicus Curiae* Google LLC in Support of Neither Party, *Chatrue*, 2026 WL 1855568; Br. for Microsoft Corp. as *Amicus Curiae* in Support of Neither Party, *Chatrue*, 2026 WL 1855568; Br. for Netchoice as *Amicus Curiae* Supporting Pet’r, *Chatrue*, 2026 WL 1855568; Brief of *Amici Curiae* of Technology Companies in Support of Neither Party, *Carpenter*, 585 U.S. 296 (2018).

There is “a growing sense of concern among consumers when it comes to their digital security,” meaning that companies that “demonstrate their commitment to user safety and privacy” will “build[] trust, gain[] customer loyalty, and foster[] a safer digital environment.”¹⁵ Where, as here, a D-Order recipient seeks to represent the interests of its users—who likely have no other recourse—they should be permitted to do so.

¹⁴ *Id.*

¹⁵ *New Deloitte Survey: Increasing Consumer Privacy and Security Concerns in the Generative AI Era*, Deloitte (Dec. 2, 2024), <https://perma.cc/D8KM-9BY4>.

CONCLUSION

For the above reasons, this Court should hold a D-Order that is overbroad or that otherwise seeks irrelevant material violates both the SCA and the Fourth Amendment's reasonableness requirement and can be quashed or modified on that basis. Additionally, this Court should recognize that users' privacy interests must be considered in assessing the reasonableness of a D-Order and whether it is unduly burdensome.

Dated: August 4, 2026

Respectfully submitted,

/s/ Nathan Freed Wessler

Nathan Freed Wessler
Laura Moraff
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500
nwessler@aclu.org

Eden B. Heilman
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF VIRGINIA
P.O. Box 26464
Richmond, VA 23261
(804) 523-2152
eheilman@acluva.org

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limits because, excluding those parts of the brief exempted under Federal Rule of Appellate Procedure 32(f), it contains 5,293 words. The brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and type-style requirements of Federal Rule of Appellate Procedure 32(a)(6) because it has been prepared in a proportionally spaced typeface (14-point Times New Roman) using Microsoft Word 365.

Dated: August 4, 2026

/s/ Nathan Freed Wessler

Nathan Freed Wessler

Counsel for *Amici Curiae*

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 4th day of August, 2026, the foregoing brief of *Amici Curiae* American Civil Liberties Union and American Civil Liberties Union of Virginia was filed electronically through the Court's CM/ECF system. Notice of this filing will be sent by e-mail to all parties by operation of the Court's electronic filing system.

Dated: August 4, 2026

/s/ Nathan Freed Wessler

Nathan Freed Wessler

Counsel for *Amici Curiae*