
New York State Supreme Court
Appellate Division – First Department

Supreme Court Index No. 30207-13

IN RE 381 SEARCH WARRANTS
DIRECTED TO FACEBOOK, INC. AND
DATED JULY 23, 2013

**NOTICE OF MOTION FOR LEAVE TO
FILE BRIEF AS PROPOSED *AMICUS CURIAE***

PERKINS COIE LLP
Jeffrey D. Vanacore
30 Rockefeller Plaza, 22nd Floor
New York, New York 10112
Telephone: (212) 262-6900
Fax: (212) 977-1649
Email: jvanacore@perkinscoie.com

Attorneys for Amici Curiae

Dated: August 8, 2014

Of Counsel:
Albert Gidari, Jr.*
Eric D. Miller*
Nicola C. Menaldo*

*Not admitted in New York
(*Pro Hac Vice Pending*)

PLEASE TAKE NOTICE that upon the annexed affirmation of Jeffrey D. Vanacore, dated August 8, 2014, Dropbox Inc., Google Inc., LinkedIn Corporation, Microsoft Corporation, Twitter, Inc., and Yelp Inc. (the “Movants”), by their attorneys Perkins Coie LLP, will move this Court, at the Supreme Court, Appellate Division, First Department, 27 Madison Avenue, New York, New York 10010, on August 18, 2014 at 10:00 a.m. or soon thereafter as counsel may be heard, for an order permitting the proposed *amici* to serve and file a brief *amici curiae*.

PLEASE TAKE NOTICE that (i) this motion relates to the New York District Attorney’s motion to dismiss also returnable on August 18, 2014 and (ii) the Movants respectfully request that this motion be heard by the same motions panel as the aforementioned motion to dismiss.

Dated: August 8, 2014

PERKINS COIE LLP

Of Counsel:
Albert Gidari, Jr.*
Eric D. Miller*
Nicola C. Menaldo*

By: 
Jeffrey D. Vanacore

30 Rockefeller Plaza
New York, New York 10112
(212) 262-6900
jvanacore@perkinscoie.com

*Not admitted in New York
(*Pro Hac Vice Pending*)

Counsel for Proposed *Amicus Curiae*

To: The New York County District Attorney's Office
Attn: Bryan Serino
1 Hogan Place
New York, NY 10013

Orin Snyder
Alexander H. Southwell
Thomas H. Dupree, Jr.
Jane Kim
Gibson, Dunn & Crutcher LLP
200 Park Avenue
New York, NY 10166-0193
Counsel for Appellants

**AFFIRMATION OF JEFFERY D. VANACORE
IN SUPPORT OF MOTION FOR LEAVE TO
FILE BRIEF AS AMICUS CURIAE**

New York State Supreme Court
Appellate Division – First Department

Supreme Court Index No. 30207-13

IN RE 381 SEARCH WARRANTS
DIRECTED TO FACEBOOK, INC. AND
DATED JULY 23, 2013

**AFFIRMATION OF JEFFERY D. VANACORE IN SUPPORT
OF MOTION FOR LEAVE TO FILE BRIEF AS *AMICUS CURIAE***

PERKINS COIE LLP
Jeffrey D. Vanacore
30 Rockefeller Plaza, 22nd Floor
Telephone: (212) 262-6900
Fax: (212) 977-1649
Email: jvanacore@perkinscoie.com

Attorneys for Amici Curiae

Dated: August 8, 2014

Of Counsel:
Albert Gidari, Jr.*
Eric D. Miller*
Nicola C. Menaldo*

*Not admitted in New York
(*Pro Hac Vice Pending*)

JEFFREY D. VANACORE, an attorney duly admitted to practice before the courts of the State of New York, affirms the following to be true under penalty of perjury:

1. I am a member in good standing of the Bar of the State of New York and counsel with the law firm of Perkins Coie LLP, attorneys for the proposed *amici*, Dropbox Inc., Google Inc., LinkedIn Corporation, Microsoft Corporation, Twitter, Inc., and Yelp Inc. This affirmation is made in support of the *Amici*'s Motion for Leave to File Brief as *Amicus Curiae* in Support of the Appellant. The *amici* have a demonstrated interest in the issues in this matter and can be of special assistance to the Court. A copy of the brief is attached hereto as Exhibit A.

2. Appellant's and Respondent's counsel have been consulted with respect to this Motion. Appellant consents to this motion; Respondent takes no position with respect to the motion.

WHEREFORE, I respectfully request that the Court grant the motion to participate in this appeal as *amici curiae*.

Dated: August 8, 2014

PERKINS COIE LLP

Of Counsel:

Albert Gidari, Jr.*

Eric D. Miller*

Nicola C. Menaldo*

*Not admitted in New York
(*Pro Hac Vice Pending*)

By: _____


Jeffrey D. Vanacore

30 Rockefeller Plaza
New York, New York 10112
(212) 262-6900
jvanacore@perkinscoie.com

Counsel for *Amici Curiae*

To: The New York County District Attorney's Office
Attn: Bryan Serino
1 Hogan Place
New York, NY 10013

Orin Snyder
Alexander H. Southwell
Thomas H. Dupree, Jr.
Jane Kim
Gibson, Dunn & Crutcher LLP
200 Park Avenue
New York, NY 10166-0193
Counsel for Appellants

EXHIBIT A

New York State Supreme Court
Appellate Division – First Department

Supreme Court Index No. 30207-13

IN RE 381 SEARCH WARRANTS
DIRECTED TO FACEBOOK, INC. AND
DATED JULY 23, 2013

**BRIEF OF *AMICI CURIAE* DROPBOX INC., GOOGLE INC.,
PINTEREST, MICROSOFT CORPORATION, TWITTER, INC., AND
YELP INC.**

PERKINS COIE LLP
Jeffrey D. Vanacore
30 Rockefeller Plaza, 22nd Floor
New York, New York 10112
Telephone: (212) 262-6900
Fax: (212) 977-1649
Email: jvanacore@perkinscoie.com

Attorneys for Amici Curiae

Dated: August 8, 2014

Of Counsel:
Albert Gidari, Jr.*
Eric D. Miller*
Nicola C. Menaldo*

*Not admitted in New York
(*Pro Hac Vice Pending*)

TABLE OF CONTENTS

	Page
STATEMENT OF INTEREST OF AMICI CURIAE	1
PRELIMINARY STATEMENT	3
ARGUMENT	6
I. A communications service provider may seek pre-execution judicial review to test the validity of an SCA warrant	6
A. This Case involves a warrant carried out by a communications service provider, not by a government official	7
B. The Fourth Amendment requires that the person executing a warrant assess its validity and challenge it if it appears invalid	9
C. The SCA prohibits providers from knowingly complying with facially invalid warrants.....	13
D. New York law does not preclude a pre-execution challenge to an SCA warrant	16
II. The permanent gag order accompanying the warrant is unlawful	17
A. The gag order violates the SCA	18
B. The gag order is an unconstitutional prior restraint	19
C. The gag order cannot satisfy strict scrutiny	20
CONCLUSION	22

TABLE OF AUTHORITIES

	Page(s)
CASES	
<i>Alexander v. United States</i> , 509 U.S. 544 (1993).....	19
<i>Application of U.S. for an Order Authorizing an In-Progress Trace of Wire Commc 'ns over Tel. Facilities</i> , 616 F.2d 1122 (9th Cir. 1980).....	8
<i>Bantam Books, Inc. v. Sullivan</i> , 372 U.S. 58 (1963).....	20
<i>Bivens v. Six Unknown Named Agents of the Fed. Bureau of Narcotics</i> , 403 U.S. 388 (1971).....	10
<i>Brown v. Entm't Merchs. Ass'n</i> , 131 S. Ct. 2729 (2011).....	20
<i>Brown v. Illinois</i> , 422 U.S. 590 (1975)	10
<i>Dickerson v. Thompson</i> , 88 A.D.3d 121 (2011).....	16
<i>Freedman v. Am. Online, Inc.</i> , 325 F. Supp. 2d 638 (E.D. Va. 2004)	13
<i>Frisby v. Schultz</i> , 487 U.S. 474 (1988).....	21
<i>Groh v. Ramirez</i> , 540 U.S. 551 (2004).....	9, 10
<i>In re Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders</i> , 562 F. Supp. 2d 876 (S.D. Tex. 2008).....	19

<i>In re Search of: 3817 W. W. End,</i> 321 F. Supp. 2d 953 (N.D. Ill. 2004)	9
<i>In re Search Warrant,</i> 193 Vt. 51, 71 A.3d 1158 (2012), <i>cert. denied</i> 133 S. Ct. 2391 (2013)	8
<i>Landmark Commc 'ns, Inc. v. Virginia,</i> 435 U.S. 829 (1978)	22
<i>Malley v. Briggs,</i> 475 U.S. 335 (1986)	10
<i>Matter of AT&T Info. Sys. v. Donohue,</i> 113 A.D.2d 395 (1985), <i>rev'd</i> , 68 N.Y.2d 821 (1986)	16
<i>Matter of Search of Info. Associated with [Redacted]@mac.com that</i> <i>is Stored at Premises Controlled by Apple, Inc.,</i> No. 14-228 (JMF), 2014 WL 1377793 (D.D.C. Apr. 7, 2014)	8
<i>Messerschmidt v. Millender,</i> 132 S. Ct. 1235 (2012)	9, 10
<i>Mills v. Alabama,</i> 384 U.S. 214 (1966)	22
<i>N.Y. Times Co. v. United States,</i> 403 U.S. 713 (1971)	20
<i>NAACP v. Button,</i> 371 U.S. 415 (1963)	21
<i>Near v. Minnesota ex rel. Olson,</i> 283 U.S. 697 (1931)	20
<i>R.A.V. v. City of St. Paul,</i> 505 U.S. 377 (1992)	22
<i>Ramirez v. Butte-Silver Bow Cnty.,</i> 298 F.3d 1022 (9th Cir. 2002), <i>aff'd sub nom. Groh v. Ramirez,</i> 540 U.S. 551 (2004)	11

<i>Reno v. ACLU</i> , 521 U.S. 844 (1997).....	20, 22
<i>United States v. Brooks</i> , 427 F.3d 1246 (10th Cir. 2005)	12
<i>United States v. Graziano</i> , 558 F. Supp. 2d 304 (E.D.N.Y. 2008)	12
<i>United States v. Grubbs</i> , 547 U.S. 90 (2006).....	11, 17
<i>United States v. Leon</i> , 468 U.S. 897 (1984).....	9, 10
<i>United States v. Playboy Entm't Grp., Inc.</i> , 529 U.S. 803 (2000).....	20
<i>United States v. Ryan</i> , 402 U.S. 530 (1971).....	15
<i>United States v. Spencer</i> , 530 F.3d 1003 (D.C. Cir. 2008).....	11
<i>United States v. Taylor</i> , 764 F. Supp. 2d 230 (D. Me. 2011).....	9
CONSTITUTIONAL PROVISIONS	
U.S. Const. amend. I	4, 5, 18, 19, 21, 22
U.S. Const. amend. IV	5, 7, 9, 12
STATUTES AND RULES	
18 U.S.C. § 2702(a).....	13
18 U.S.C. § 2702(a)(3).....	6
18 U.S.C. § 2702(b).....	13
18 U.S.C. § 2703.....	6

18 U.S.C. § 2703(a).....	6, 13
18 U.S.C. § 2703(d)	15, 16
18 U.S.C. § 2703(e).....	14
18 U.S.C. § 2703(g)	8
18 U.S.C. § 2705(b)	18
18 U.S.C. § 2707	13
18 U.S.C. § 2707(e).....	14
18 U.S.C. § 3105	7
42 U.S.C. § 1983	10
Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (18 U.S.C. §§ 2701-2712)	6
Stored Communications Act, 18 U.S.C. §§ 2701-2712.....	passim
N.Y. Crim. Proc. Law § 690.05(2).....	7
N.Y. Crim. Proc. Law § 690.10	6
N.Y. Crim. Proc. Law § 690.25(1).....	7
N.Y. Crim. Proc. Law § 710.40(1).....	16
Fed. R. Crim. P. 41.....	6
OTHER AUTHORITIES	
Paul K. Ohm, <i>Parallel-Effect Statutes and E-Mail “Warrants”: Reframing the Internet Surveillance Debate</i> , 72 Geo. Wash. L. Rev. 1599 (2004).....	8

STATEMENT OF INTEREST OF *AMICI CURIAE*

Dropbox Inc. provides file storage, synchronization and collaboration services. Google Inc. is a diversified technology company whose mission is to organize the world's information and make it universally accessible and useful. Google offers a variety of web-based products and services—including Search, Gmail, Google+, Maps, YouTube, and Blogger—that are used by people throughout the United States and around the world. Microsoft Corporation is a provider of electronic communication services and remote computing storage services to individual users, enterprises, educational institutions, and governments worldwide. Pinterest provides an online tool for people to collect, organize, and share the things and places they love. Twitter, Inc. is a global platform for public self-expression where any user can create a Tweet and any user can follow other users. Twitter's mission is to give everyone the power to create and share ideas and information instantly, without barriers. Yelp Inc. operates Yelp.com and related websites and mobile applications worldwide that allow members of the public, free of charge, to read and write reviews about local businesses, government services, and other establishments.

This case involves a challenge to a search warrant compelling the disclosure of all data associated with 381 Facebook users' accounts and permanently prohibiting Facebook from notifying the affected users. *Amici curiae* regularly

receive search warrants and related legal requests from federal, state, and local law enforcement. Because *amici* are committed to user privacy, they carefully scrutinize legal process they receive to ensure that it complies with the law. When such process is ambiguous, inaccurate, overbroad, or unduly burdensome, or when there are questions about whether the process complies with the statute or is otherwise constitutional, *amici* reject the legal process or require law enforcement to correct the problem. In addition, because *amici* believe that users should be able to know and understand as much as possible about the number and types of requests providers receive, some of the *amici* publish regular transparency reports containing aggregate information about such requests.

Some *amici* have challenged warrants in court before. Although many such challenges are brought under seal and typically result in orders that are not publicly available, courts have entertained those challenges, especially when the issues affect the rights of users to be secure in the content of their communications stored online. *Amici* will bring such challenges in the future to protect user data from indiscriminate warrants such as those at issue here. *Amici* therefore have a strong interest in the resolution of the issues in this case.

PRELIMINARY STATEMENT

This case arises from the largest set of search warrants that Facebook has ever received. The New York County District Attorney directed Facebook to collect and disclose virtually all communications, data, and information from 381 Facebook accounts. The warrants contained perpetual nondisclosure provisions, barring Facebook from ever informing its users about the warrants. Facebook moved to quash the warrants, but the trial court denied the motion. Facebook has now appealed.

This appeal presents important and recurring questions of constitutional law. Facebook has addressed the constitutional issues in its opening brief, and *amici* share in those views. In particular, *amici* agree with Facebook that a provider that receives a search warrant has third-party standing to raise the constitutional rights of its subscribers. That is especially so where, as here, the provider is subject to a nondisclosure or “gag” order. Only 62 of the Facebook users targeted by the warrants in this case have been charged with a crime. The other 319 users have had their personal information seized and, under the government’s view of the law, would never know that the government has obtained that information and continues to possess it long after the government has concluded its investigation. Unless Facebook is able to assert its subscribers’ constitutional rights—and any of its own rights—the legality of the government’s

actions with respect to those subscribers will escape review altogether. And had the government chosen to indict no one, no one would have been the wiser.

In this brief, *amici* focus on two issues of particular importance under the Stored Communications Act (“SCA”), 18 U.S.C. §§ 2701-2712. First, the government has suggested that a warrant, unlike a subpoena, is not subject to pre-execution judicial review. While that may be true of a warrant executed by a law-enforcement officer, it is not true of a warrant that is fulfilled by a communications service provider under the SCA. It is well settled that the person executing a warrant must confirm the facial validity of the warrant and is subject to civil liability for failing to do so. Pre-execution judicial review is necessary to allow providers to discharge their responsibility to decline to fulfill warrants that appear to be invalid. And the SCA’s civil liability and immunity provisions make clear that Congress contemplated that such review would be available.

Second, the gag order accompanying the warrant violates both the SCA and the First Amendment. The SCA allows a warrant to prohibit disclosure, but only for a limited period. And the First Amendment requires that any content-based restriction on speech be narrowly tailored to serve a compelling government interest. A disclosure prohibition such as the one here, which contains no time limit whatsoever, is the antithesis of narrow tailoring.

As this case illustrates, the combination of the government's Fourth Amendment theory and its First Amendment theory is particularly troubling. Under the government's theory, a provider would have no recourse to question the validity of a warrant issued under the SCA. And under the government's theory, a provider would have no mechanism to challenge a perpetual gag order preventing it from speaking about the warrant it receives. Even if the warrant demanded all content from every user account worldwide, the provider would have no standing to complain. No defect or error in the warrant could be raised; the provider would be required to comply while ignoring the warrant's invalidity, no matter how obvious. And because the subscribers would be prohibited from learning about the warrant, they would not be able to challenge it either. That result is contrary to the law, and this Court should reject it.

Even setting aside the structure of the SCA, common sense dictates that service providers must be able to challenge invalid legal process directed to their users' information. Users trust services like *amici*'s to safeguard their information. That trust would be eroded by a rule stating that providers had no forum in which to challenge unlawful government demands for information. At bottom, the service of an illegal data demand on a provider causes an injury to the provider itself for which the law must provide a remedy.

ARGUMENT

I. A COMMUNICATIONS SERVICE PROVIDER MAY SEEK PRE-EXECUTION JUDICIAL REVIEW TO TEST THE VALIDITY OF AN SCA WARRANT

The warrants in this litigation are governed by the Stored Communications Act, passed as part of the Electronic Communications Privacy Act of 1986 (“ECPA”), Pub. L. No. 99-508, 100 Stat. 1848, and codified at 18 U.S.C. §§ 2701-2712; *see* A5 (trial court order relying on the SCA as a source of authority for issuing the warrants). The SCA generally prohibits providers from disclosing certain customer communications and records to law enforcement, but it contains an exception for cases in which the disclosure is as authorized by a subpoena, a court order, or a warrant. 18 U.S.C. §§ 2702(a)(3), 2703. Where the government uses a warrant to compel disclosure, the SCA requires that it be supported by probable cause. 18 U.S.C. § 2703(a) (requiring that warrant be issued using the procedures under federal or state criminal procedure); Fed. R. Crim. P. 41 (requiring that warrants be supported by probable cause); N.Y. Crim. Proc. Law § 690.10 (same).

The government has argued that a search warrant is not an appealable order. In its view, because a warrant, unlike a subpoena, has already been reviewed by a magistrate before it is issued, there is no need to provide an opportunity for further judicial review before the warrant is executed. That

argument ignores the context of warrants served on providers under the SCA, which are generally carried out not by the police, but by communications providers themselves. In that context, both the Fourth Amendment and the SCA require that the provider have an opportunity for pre-execution judicial review.

A. This Case involves a warrant carried out by a communications service provider, not by a government official

Ordinarily, a warrant authorizing a physical search is served and executed by one of the officers mentioned in the warrant, or by an officer otherwise authorized by law. N.Y. Crim. Proc. Law § 690.05(2) (“A search warrant is a court order and process directing a police officer to conduct . . . a search.”); *id.* § 690.25(1) (“A search warrant must be addressed to a police officer whose geographical area of employment embraces or is embraced or partially embraced by the county of issuance.”); *accord* 18 U.S.C. § 3105 (“A search warrant may in all cases be served by any of the officers mentioned in its direction or by an officer authorized by law to serve such warrant, but by no other person, except in aid of the officer on his requiring it, he being present and acting in its execution.”). An officer may require another person to aid in executing the warrant, but generally the officer must be present. In practice, that means that officers conduct searches pursuant to warrants supported by affidavits that they themselves prepared and for which they have established probable cause.

By contrast, when a warrant is served on an online provider under the SCA, the provider is expected to fulfill its obligations under the SCA, even without an officer present. 18 U.S.C. § 2703(g) (“[T]he presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter”). Generally, a warrant is sent via fax or email to the provider that is the subject of the warrant, and the provider is charged with finding the specified content and sending it to the officer. *See* Paul K. Ohm, *Parallel-Effect Statutes and E-Mail “Warrants”*: *Reframing the Internet Surveillance Debate*, 72 *Geo. Wash. L. Rev.* 1599, 1611-12 (2004). Under that regime, “no confrontation between government and citizen takes place.” *Application of U.S. for an Order Authorizing an In-Progress Trace of Wire Commc’ns over Tel. Facilities*, 616 F.2d 1122, 1130 (9th Cir. 1980).

Providers search for responsive data as directed in the warrant. *See, e.g., Matter of Search of Info. Associated with [Redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.*, No. 14-228 (JMF), 2014 WL 1377793, at *6 (D.D.C. Apr. 7, 2014) (requiring the third party service provider to “perform the search at the government’s request and turn over any relevant data that it discovers”); *In re Search Warrant*, 193 Vt. 51, 71 A.3d 1158, 1180 (2012) (third parties are permitted to assist in the execution of search warrants) (citing cases), *cert. denied*, 133 S. Ct. 2391 (2013). Providers are expected to seize the records

subject to the warrant and turn them over to law enforcement for searching. *See, e.g., United States v. Taylor*, 764 F. Supp. 2d 230, 237 (D. Me. 2011) (“The Fourth Amendment does not require the government to delegate a prescreening function to the internet service provider or to ascertain which e-mails are relevant before copies are obtained from the internet service provider for subsequent searching.”); *In re Search of: 3817 W. W. End*, 321 F. Supp. 2d 953, 958 (N.D. Ill. 2004) (“It is frequently the case with computers that the normal sequence of ‘search’ and then selective ‘seizure’ is turned on its head”). In other words, providers are charged with interpreting the scope of a warrant, identifying the places and data to be searched and items to be seized, and turning over that information to law enforcement.

B. The Fourth Amendment requires that the person executing a warrant assess its validity and challenge it if it appears invalid

The United States Supreme Court has held that “[i]t is incumbent on the officer executing a search warrant to ensure the search is lawfully authorized and lawfully conducted.” *Groh v. Ramirez*, 540 U.S. 551, 563 (2004). As the Court has explained, “the fact that a neutral magistrate has issued a warrant” generally indicates that officers executing that warrant have “acted in an objectively reasonable manner.” *Messerschmidt v. Millender*, 132 S. Ct. 1235, 1245 (2012); *see United States v. Leon*, 468 U.S. 897, 922-923 (1984). The presence of a warrant, however, “does not end the inquiry into objective reasonableness.”

Messerschmidt, 132 S. Ct. at 1245. Instead, the Court has recognized that officers may still be civilly liable—in an action under 42 U.S.C. § 1983 or *Bivens v. Six Unknown Named Agents of the Federal Bureau of Narcotics*, 403 U.S. 388 (1971)—for conducting a search authorized by a warrant in circumstances where “it is obvious that no reasonably competent officer would have concluded that a warrant should issue.” *Malley v. Briggs*, 475 U.S. 335, 341 (1986). For example, officers may be subject to liability for conducting a search pursuant to a warrant that is “based on an affidavit ‘so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable’” or pursuant to a warrant that is “so facially deficient—*i.e.*, in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid.” *Leon*, 468 U.S. at 923 (quoting *Brown v. Illinois*, 422 U.S. 590, 610-11 (1975) (Powell, J., concurring in part)); *see Messerschmidt*, 132 S. Ct. at 1245; *see also Groh*, 540 U.S. at 563 (unreasonable to rely on warrant that failed to contain particularized description of things to be seized).

Often, the officer executing a warrant will be the same officer who applied for the warrant and thus will have been able to address concerns about its validity at that time. In other cases in which an officer executing a warrant doubts its validity, he or she can return to the issuing magistrate to seek a revised warrant, supported, if necessary, by a revised affidavit establishing probable cause. *See*,

e.g., *Ramirez v. Butte-Silver Bow Cnty.*, 298 F.3d 1022, 1026 (9th Cir. 2002) (concluding that an officer lacked qualified immunity for executing a facially defective warrant, and explaining that “[t]he only way [the officer] could have remedied the defect in the warrant was to ask a magistrate to issue a corrected version”), *aff’d sub nom. Groh v. Ramirez*, 540 U.S. 551 (2004); *see also United States v. Spencer*, 530 F.3d 1003, 1008 (D.C. Cir. 2008) (“[W]hen officers learn of new facts that negate probable cause, they may not rely on an earlier-issued warrant but instead must return to the magistrate”) (emphasis omitted).

When a communications service provider, rather than an officer, is charged with carrying out the warrant, the provider must have a similar mechanism for challenging the warrant’s validity. Judicial review provides a mechanism that is analogous to the mechanism available to officers of returning to the magistrate and seeking modification of the warrant.

The need for some means of challenging warrants is particularly acute in the context of searches of electronically stored data because of the potential for ambiguity in specifying how the search is to be conducted and what things are to be gathered. In the context of a physical search, relatively little specificity as to the manner of execution may be required: the executing officer generally knows what he or she is looking for. *See United States v. Grubbs*, 547 U.S. 90, 97-98 (2006) (“Nothing in the language of the Constitution or in th[e] [Supreme] Court’s

decisions interpreting that language suggests that, in addition to the requirements set forth in the text [of the Fourth Amendment], search warrants also must include a specification of the precise manner in which they are to be executed.”) (internal quotation marks and citation omitted); *United States v. Brooks*, 427 F.3d 1246, 1251 (10th Cir. 2005) (“This court has never required warrants to contain a particularized computer search strategy.”); *United States v. Graziano*, 558 F. Supp. 2d 304, 315-16 (E.D.N.Y. 2008) (collecting cases). In the SCA context, however, where no officer is present, a lack of specificity can easily result in a search that is insufficiently particularized. That is especially so because law enforcement is often unfamiliar with providers’ platforms and technologies, which involve many different services and which may store data in many locations, including outside the United States. In the experience of *amici*, law enforcement sometimes sends the same boilerplate language to different providers, notwithstanding the differences among their platforms. Indeed, law enforcement often uses warrants to compel information that simply does not exist or cannot be obtained using a provider’s existing systems or capabilities. Where a provider is unable to reach a resolution directly with law enforcement on these issues, there must be a means to petition a judicial officer to adjudicate the dispute.

Providers receive warrants from the federal government, from all 50 states and numerous United States territories, and from local government entities across

the country. Each jurisdiction uses a different form, creating a heightened possibility for ambiguity and uncertainty as to what is covered by the warrant. *See Freedman v. Am. Online, Inc.*, 325 F. Supp. 2d 638, 649-50 (E.D. Va. 2004) (noting that the provider received warrants “from jurisdictions all over the country that use different forms and procedures”); 18 U.S.C. § 2703(a) (requiring that a warrant issued under the SCA comply with the Federal Rules of Criminal Procedure or comparable state warrant procedures). In most cases, providers can resolve ambiguities and seek clarification through dialogue with law enforcement. But when that dialogue fails, the law must provide a remedy.

C. The SCA prohibits providers from knowingly complying with facially invalid warrants

The SCA categorically prohibits providers from divulging the contents of a communication to a government entity except under legal process as explicitly provided in the statute. 18 U.S.C. §§ 2702(a), (b). A provider that knowingly violates the prohibition on disclosing its users’ electronic communications to the government is subject to a civil action for damages. *Id.* § 2707. The SCA’s prohibition and civil liability provisions demonstrate that Congress contemplated that providers could challenge facially invalid warrants before complying with them.

As relevant here, the SCA contains two provisions immunizing providers from liability for complying with a warrant. First, Section 2703(e) states that “[n]o

cause of action shall lie in any court against any provider . . . for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.” 18 U.S.C. § 2703(e). Second, Section 2707(e) provides that “[a] good faith reliance on . . . a court warrant or order . . . is a complete defense to any civil or criminal action” under the SCA. 18 U.S.C. § 2707(e).

Section 2707(e) provides immunity for “good faith reliance” on a warrant. If a provider determines that a warrant or subpoena is facially invalid, it must be able to challenge that process in court. Otherwise, it would be put on the horns of a dilemma: comply with the invalid process and risk forfeiting its immunity, or refuse to comply and face coercive sanctions. The good faith immunity would make little sense if providers were required to comply with all legal process, no matter how obviously defective. A provider, for example, would not implement a wiretap on an ordinary federal warrant that lacked the appropriate findings for a wiretap order, but under the government’s theory, the provider would have no right to challenge such process. One might hope that no court would issue such process, but the SCA is a complicated statute, and *amici* have received orders with facial deficiencies.

Congress clearly intended that providers be able to avoid complying with court orders, including warrants, where they cannot do so in good faith. And, just

as clearly, Congress did not intend for providers to risk contempt of court in order to comply with their statutory obligations. *See United States v. Ryan*, 402 U.S. 530, 533 (1971) (“[A] custodian [of records] could hardly [be] expected to risk a citation for contempt in order to secure . . . an opportunity for judicial review.”). The limitations on the immunity provision of the SCA make it clear that providers charged with fulfilling a search warrant must have the right to seek corrective action in a judicial forum before the warrant is executed.

As the government noted in the trial court, the SCA authorizes providers to move to quash or amend legal process in the case of unusually voluminous records and otherwise burdensome requests. 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, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.”). But that provision does not mean that providers cannot also challenge a warrant on the ground that it is ambiguous, invalid, or illegal. To the contrary, because compliance with a facially invalid warrant could potentially subject a provider to civil liability, compliance in those circumstances would constitute an “undue burden.” Thus, Section 2703(d) confirms that SCA warrants, unlike ordinary warrants directed to law-enforcement officers, are subject to pre-execution judicial review.

D. New York law does not preclude a pre-execution challenge to an SCA warrant

Because the SCA contemplates that providers will be able to bring pre-execution challenges to warrants, any provision of state law that prohibited such challenges would be preempted. In any event, no provision of state law prohibits judicial review in this context. To the contrary, as a court of general jurisdiction, the Supreme Court of New York has authority to fashion a remedy appropriate to a challenge to a defective warrant. *See Dickerson v. Thompson*, 88 A.D.3d 121, 123-24 (2011) (“[E]ven in the absence of any direct grant of legislative power Supreme Court has the ‘inherent authority . . . to fashion whatever remedies are required for the resolution of justiciable disputes and the protection of the rights of citizens.’”) (quoting *Matter of AT&T Info. Sys. v. Donohue*, 113 A.D.2d 395, 400 (1985), *rev’d on other grounds*, 68 N.Y.2d 821 (1986)).

In the trial court, the government relied on New York Criminal Procedure Law § 710.40(1), which provides that “[a] motion to suppress evidence must be made after the commencement of the criminal action in which such evidence is allegedly about to be offered.” That provision is inapplicable here because a motion to quash or amend a warrant under the SCA is not a motion to suppress evidence; it is a motion made by the party carrying out a warrant to ensure that the strictures of the SCA have been met before turning over evidence to the government.

Nor is the government's position supported by case law rejecting the availability of a pre-execution remedy for defective warrants in the context of physical searches. In *Grubbs*, the United States Supreme Court noted, in dicta, that “[t]he Constitution protects property owners not by giving them license to engage the police in a debate over the basis for the warrant, but by interposing, *ex ante*, the ‘deliberate, impartial judgment of a judicial officer . . . between the citizen and the police,’ and by providing, *ex post*, a right to suppress evidence improperly obtained and a cause of action for damages.” 547 U.S. at 99 (internal quotation marks and citation omitted). But unlike a citizen who is under investigation—who will have the opportunity to challenge the warrant in a suppression hearing after he is indicted—a third-party provider who receives a warrant has no post-execution suppression remedy. Moreover, as explained above, a provider carries out an SCA warrant without an officer present, and a provider necessarily must view the warrant before it does so. Nothing in *Grubbs*, or any other decision of the Court, casts doubt on the availability of a pre-execution remedy to allow the third party charged with fulfilling the warrant to obtain judicial review of its validity.

II. THE PERMANENT GAG ORDER ACCOMPANYING THE WARRANT IS UNLAWFUL

Because a subscriber who is unaware of a search will be unable to challenge it, the ability of providers to challenge a defective warrant is particularly

important when the warrant requires delayed notice to the subscriber. In this case, however, the broad warrant was accompanied by an even broader gag order that does not merely delay notice but prohibits it indefinitely. That order violates both the SCA and the First Amendment.

A. The gag order violates the SCA

Under 18 U.S.C. § 2705(b), a court may command an electronic communications service provider to delay notice of a warrant to a subscriber “for such period as the court deems appropriate,” but only if the court determines that notice will result in

- (1) endangering the life or physical safety of an individual;
- (2) flight from prosecution;
- (3) destruction of or tampering with evidence;
- (4) intimidation of potential witnesses; or
- (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

Id. § 2705(b). The statute’s use of the word “period” demonstrates that such an order must last for a limited time. But even without that limitation, the five enumerated factors, all of which are tied to an ongoing investigation, compel the same conclusion. Once the existence and targets of the investigation are no longer a secret, there is no reason to believe that the disclosure of the warrant could cause any of the enumerated harms; certainly the trial court articulated no reason to think that such harms could result. Accordingly, the permanent gag order is contrary to the SCA. *See In re Sealing & Non-Disclosure of Pen/Trap/2703(d)*

Orders, 562 F. Supp. 2d 876, 895 (S.D. Tex. 2008) (“As a rule, sealing and non-disclosure of electronic surveillance [demands] must be neither permanent nor, what amounts to the same thing, indefinite.”).

B. The gag order is an unconstitutional prior restraint

Even if the SCA permitted an order such as the one entered here, the order would be contrary to the First Amendment because it is an unlawful prior restraint. In *Alexander v. United States*, 509 U.S. 544 (1993), the United States Supreme Court explained that “[t]he term prior restraint is used to describe administrative and judicial orders forbidding certain communications when issued in advance of the time that such communications are to occur.” *Id.* at 550 (emphasis omitted) (internal quotation marks and citation omitted). That is precisely what the gag order in this case does, and the order is therefore appropriately characterized as a prior restraint. “Any system of prior restraints of expression,” the Supreme Court has held, is subject to “a heavy presumption against its constitutional validity.” *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 70 (1963); see *Near v. Minnesota ex rel. Olson*, 283 U.S. 697, 716 (1931). As explained more fully below, the gag order here cannot satisfy ordinary strict scrutiny. *A fortiori*, it is insufficient to justify a prior restraint. See *N.Y. Times Co. v. United States*, 403 U.S. 713, 730 (1971) (Stewart, J., concurring) (reversing injunction against publication of the Pentagon Papers because “I cannot say that

disclosure of any of them will *surely* result in direct, immediate, and irreparable damage to our Nation or its people”) (emphasis added).

C. The gag order cannot satisfy strict scrutiny

As a content-based restriction on speech, the gag order is invalid unless the government “can demonstrate that it passes strict scrutiny—that is, unless it is justified by a compelling government interest and is narrowly drawn to serve that interest.” *Brown v. Entm’t Merchs. Ass’n*, 131 S. Ct. 2729, 2738 (2011). The narrow-tailoring component of that test requires the government to show that there are no “less restrictive alternatives [that] would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve.” *Reno v. ACLU*, 521 U.S. 844, 874 (1997). Under the strict-scrutiny standard, “[i]t is rare that a regulation restricting speech because of its content will ever be permissible.” *United States v. Playboy Entm’t Grp., Inc.*, 529 U.S. 803, 818 (2000).

It is far from clear that the order in this case serves a compelling interest. The trial court stated that “disclosure by Facebook of the underlying search warrants to the targeted account holders would *potentially* have dire direct and indirect consequences,” and it noted that evidence “*could be* destroyed, removed or deleted,” that suspects or witnesses “*could* flee or be intimidated,” and that the integrity of the investigation “*could be* severely compromised.” A7 (emphasis

added). The potential for such harms can be imagined in every case. But without some reason to believe that the harms are *likely* to result from disclosure, the interest in preventing them cannot reasonably be described as compelling. While there may such a reason in this case, the trial court failed to articulate it.

In any event, even assuming that the gag order serves a compelling government interest, it is not narrowly tailored to protect that interest. Specifically, its indefinite duration means that its temporal scope is not tailored at all. Whatever harm might result from the disclosure of the warrant now, that harm will no longer exist once the individuals whose information is sought by the warrant have been indicted and the existence of the investigation has been revealed. The order therefore violates the First Amendment. *See Frisby v. Schultz*, 487 U.S. 474, 485 (1988) (narrow tailoring is satisfied “only if each activity within the proscription’s scope is an appropriately targeted evil”); *NAACP v. Button*, 371 U.S. 415, 438 (1963) (“Broad prophylactic rules in the area of free expression are suspect.”).

The highly restrictive nature of the gag order further demonstrates that it cannot be the least restrictive means of achieving the government’s asserted objective. *See Reno*, 521 U.S. at 874. The order broadly prohibits speech on matters of vital public concern—namely, the government’s exercise of coercive authority to obtain subscriber information *en masse* from a communications

service provider. *See Mills v. Alabama*, 384 U.S. 214, 218 (1966) (“Whatever differences may exist about interpretations of the First Amendment, there is practically universal agreement that a major purpose of that Amendment was to protect the free discussion of governmental affairs.”); *accord Landmark Commc’ns, Inc. v. Virginia*, 435 U.S. 829, 838-39 (1978). The government’s gathering of information from electronic communications providers has been a subject of considerable public debate, and orders such as the one at issue here impermissibly suppress the speech of those online service providers who might be best positioned to offer an informed perspective on the government’s position. The First Amendment does not permit the government to silence a key participant in a debate about the government’s activities. *R.A.V. v. City of St. Paul*, 505 U.S. 377 (1992).

CONCLUSION

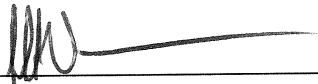
This Court should reverse the decision below and quash the warrants.

Respectfully submitted.

Dated: August 8, 2014

PERKINS COIE LLP

Of Counsel:
Albert Gidari, Jr.*
Eric D. Miller*
Nicola C. Menaldo*

By: 
Jeffrey D. Vanacore

30 Rockefeller Plaza
New York, New York 10112
(212) 262-6900
jvanacore@perkinscoie.com

*Not admitted in New York
(*Pro Hac Vice Pending*)

Counsel for *Amici Curiae*

PRINTING SPECIFICATION STATEMENT

I hereby certify pursuant to 22 N.Y. C.R.R. § 600.10(d)(1)(v) that this brief was prepared, using Microsoft Office Word 2010, to the following specifications:

Typeface: Times New Roman, a proportionally spaced typeface

Point size: 14

Line-spacing: Double, in accordance with Rule 500.1(l)

Word Count: The body of this brief, inclusive of point headings and footnotes, and exclusive of those pages containing the table of contents, the table of authorities, the proof of service and this Statement, contains 5180 words.


Dated: New York, New York
August 8, 2014

Respectfully submitted,

PERKINS COIE LLP

Of Counsel:
Albert Gidari, Jr.*
Eric D. Miller*
Nicola C. Menaldo*

*Not admitted in New York
(*Pro Hac Vice Pending*)

By: 
Jeffrey D. Vanacore

30 Rockefeller Plaza
New York, New York 10112
(212) 262-6900
jvanacore@perkinscoie.com

Counsel for Proposed *Amicus Curiae*

SUPREME COURT OF THE STATE OF NEW YORK
APPELLATE DIVISION: FIRST DEPARTMENT

IN RE 381 SEARCH WARRANTS
DIRECTED TO FACEBOOK, INC. AND
DATED JULY 23, 2013

Index No.: 30207-13

AFFIDAVIT OF SERVICE

STATE OF NEW YORK)
 : ss:
COUNTY OF NEW YORK)

I, NELSON VARGAS, being duly sworn, deposes and says:


1. I am not a party to this action, am over 18 years of age, and reside in Queens County, New York.

2. On August 8, 2014, I served a true and correct copy of the **NOTICE OF MOTION FOR LEAVE TO FILE BRIEF AS PROPOSED AMICUS CURIAE and AFFIRMATION OF JEFFERY D. VANACORE IN SUPPORT OF MOTION FOR LEAVE TO FILE BRIEF AS AMICUS CURIAE with EXHIBIT A- BRIEF OF AMICI CURIAE DROPBOX INC., GOOGLE INC., PINTEREST, MICROSOFT CORPORATION, TWITTER, INC., AND YELP INC.** on the following by e-mail on consent:

The New York County District Attorney's Office
Attn: Bryan Serino
1 Hogan Place
New York, NY 10013

and

Orin Snyder
Alexander H. Southwell
Thomas H. Dupree, Jr.
Jane Kim
Gibson, Dunn & Crutcher LLP
200 Park Avenue
New York, NY 10166-0193
Counsel for Appellants


NELSON VARGAS

Sworn to before me this
8th day of August 2014

JEFFREY D. VANACORE
Notary Public, State of New York
No. 02VA6089963
Qualified in New York County
Commission Expires April 30, 2015



Notary Public