

Court of Appeals of the State of New York

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

FACEBOOK, INC.,

Appellant,

– against –

NEW YORK COUNTY DISTRICT ATTORNEY'S OFFICE,

Respondent.

IN THE MATTER OF THE MOTION TO COMPEL DISCLOSURE OF THE SUPPORTING
AFFIDAVIT RELATING TO CERTAIN SEARCH WARRANTS DIRECTED TO
FACEBOOK, INC., DATED JULY 23, 2013

FACEBOOK, INC.,

Appellant,

– against –

NEW YORK COUNTY DISTRICT ATTORNEY'S OFFICE,

Respondent.

**NOTICE OF MOTION FOR LEAVE TO FILE BRIEF OF AMAZON.COM, INC.,
APPLE INC., BOX, INC., DROPBOX INC., GOOGLE INC., MICROSOFT
CORPORATION, MOZILLA CORPORATION, NEST LABS, INC., NIANTIC,
INC., PINTEREST, INC., RED HAT INC., REDDIT, INC., SNAP INC., AND
TWITTER INC. AS *AMICI CURIAE* IN SUPPORT OF APPELLANT**

JEFFREY LANDIS
ZwillGen PLLC
1900 M Street NW, Suite 250
Washington, DC 20036
Counsel for Apple Inc.

DAVID B. PERRY
RED HAT INC.
100 East Davie Street
Raleigh, NC 27601
Counsel for Red Hat Inc.

JEFFREY D. VANACORE
Counsel of Record
ERIC D. MILLER, TODD M.
HINNEN, ERIN K. EARL
PERKINS COIE LLP
30 Rockefeller Plaza
New York, New York 10112
Tel.: (212) 262-6900
Fax: (212) 399-8021
*Counsel for Amazon.com, Inc.,
Box, Inc., Dropbox Inc.,
Google Inc., Microsoft
Corp., Mozilla Corp., Nest
labs, Inc., Niantic, Inc.,
Pinterest, Inc., Reddit, Inc.,
Snap Inc., and Twitter Inc.*

PLEASE TAKE NOTICE that upon the annexed affirmation of Jeffrey D. Vanacore, dated December 30, 2016, Amazon.com, Inc., Apple Inc., Box, Inc., Dropbox Inc., Google Inc., Microsoft Corporation, Mozilla Corporation, Nest Labs, Inc., Niantic, Inc., Pinterest, Inc., Red Hat Inc., Reddit, Inc., Snap Inc., and Twitter Inc. (“Movants”), by their attorneys, will move this Court, at the Court of Appeals of the State of New York, at 20 Eagle Street, Albany, New York, 12207, on January 7, 2017, at 10:00 a.m. or as soon thereafter as counsel may be heard, for an order permitting the proposed *amici* to serve and file a brief *amici curiae*.

Dated: December 30, 2016

PERKINS COIE LLP

Of Counsel:
Eric D. Miller*
Todd M. Hinnen*
Erin K. Earl*

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

By: Jeffrey D. Vanacore / TMH
Jeffrey D. Vanacore
30 Rockefeller Plaza
New York, New York 10112
Tel.: (212) 262-6900
Fax: (212) 399-8021
jvanacore@perkinscoie.com
Counsel for Proposed *Amici Curiae* Amazon.com, Inc., Box, Inc., Dropbox Inc., Google Inc., Microsoft Corporation, Mozilla Corporation, Nest Labs, Inc., Niantic, Inc., Pinterest, Inc., Reddit, Inc., Snap, Inc., and Twitter Inc.

Dated: December 30, 2016

APPLE INC.

By: Jeffrey Landis
Jeffrey Landis
ZwillGen PLLC
1900 M Street NW, Suite 250
Washington, DC 20036
jeff@zwillgen.com
202-706-5203
Counsel for Proposed *Amicus Curiae* Apple Inc.

Dated: December 30, 2016

RED HAT INC.

By: _____
David B. Perry
100 East Davie Street
Raleigh, NC 27601
dperry@redhat.com
Counsel for Proposed *Amicus Curiae* Red Hat Inc.

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.
Gabriel K. Gillett
Gibson, Dunn & Crutcher LLP
200 Park Avenue
New York, NY 10166-0193
Counsel for Appellants

Of Counsel:
Eric D. Miller*
Todd M. Hinnen*
Erin K. Earl*

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

By: _____
Jeffrey D. Vanacore
30 Rockefeller Plaza
New York, New York 10112
Tel.: (212) 262-6900
Fax: (212) 399-8021
jvanacore@perkinscoie.com
Counsel for Proposed *Amici Curiae* Amazon.com, Inc.,
Box, Inc., Dropbox Inc.,
Google Inc., Microsoft
Corporation, Mozilla
Corporation, Nest Labs,
Inc., Niantic, Inc., Pinterest,
Inc., Reddit, Inc., Snap, Inc.,
and Twitter Inc.


Dated: December 30, 2016

APPLE INC.

By: _____
Jeffrey Landis
ZwillGen PLLC
1900 M Street NW, Suite 250
Washington, DC 20036
jeff@zwillgen.com
202-706-5203
Counsel for Proposed *Amicus Curiae* Apple Inc.

Dated: December 30, 2016

RED HAT INC

By: _____

David B. Perry
100 East Davie Street
Raleigh, NC 27601
dperry@redhat.com
Counsel for Proposed *Amicus Curiae* Red Hat Inc.

To: The New York County District Attorney's Office

Court of Appeals of the State of New York

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

FACEBOOK, INC.,

Appellant,

– against –

NEW YORK COUNTY DISTRICT ATTORNEY'S OFFICE,

Respondent.

IN THE MATTER OF THE MOTION TO COMPEL DISCLOSURE OF THE SUPPORTING
AFFIDAVIT RELATING TO CERTAIN SEARCH WARRANTS DIRECTED TO
FACEBOOK, INC., DATED JULY 23, 2013

FACEBOOK, INC.,

Appellant,

– against –

NEW YORK COUNTY DISTRICT ATTORNEY'S OFFICE,

Respondent.

**AFFIRMATION OF JEFFREY D. VANACORE IN SUPPORT OF MOTION FOR
LEAVE TO FILE BRIEF OF AMAZON.COM, INC., APPLE INC., BOX, INC.,
DROPBOX INC., GOOGLE INC., MICROSOFT CORPORATION, MOZILLA
CORPORATION, NEST LABS, INC., NIANTIC, INC., PINTEREST, INC., RED
HAT INC., REDDIT, INC., SNAP INC., AND TWITTER INC. AS *AMICI CURIAE*
IN SUPPORT OF APPELLANT**

JEFFREY LANDIS
ZwillGen PLLC
1900 M Street NW, Suite 250
Washington, DC 20036
Counsel for Apple Inc.

DAVID B. PERRY
RED HAT INC.
100 East Davie Street
Raleigh, NC 27601
Counsel for Red Hat Inc.

JEFFREY D. VANACORE
Counsel of Record
ERIC D. MILLER, TODD M.
HINNEN, ERIN K. EARL
PERKINS COIE LLP
30 Rockefeller Plaza
New York, New York 10112
Tel.: (212) 262-6900
Fax: (212) 399-8021
*Counsel for Amazon.com, Inc.,
Box, Inc., Dropbox Inc.,
Google Inc., Microsoft
Corporation, Mozilla
Corporation, Nest labs,
Inc., Niantic, Inc.,
Pinterest, Inc., Reddit, Inc.,
Snap Inc., and Twitter Inc.*

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*, Amazon.com, Inc., Box, Inc., Dropbox Inc., Google Inc., Mozilla Corporation, Nest Labs, Inc., Niantic, Inc., Pinterest, Inc., Reddit Inc., Snap Inc., and Twitter Inc. I and the undersigned counsel make this affirmation in support of *Amici's* Motion for Leave to File Brief as *Amici 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, which is 6,968 words, is attached hereto as Exhibit A.

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

Dated: December 30, 2016

Of Counsel:
Eric D. Miller*
Todd M. Hinnen*
Erin K. Earl*

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

PERKINS COIE LLP

By: Jeffrey D. Vanacore /TMH
Jeffrey D. Vanacore
30 Rockefeller Plaza
New York, New York 10112
Tel.: (212) 262-6900
Fax: (212) 399-8021
jvanacore@perkinscoie.com
Counsel for Proposed *Amici*
Curiae Amazon.com, Inc., Box,
Inc., Dropbox Inc., Google Inc.,
Microsoft Corporation, Mozilla
Corporation, Nest Labs, Inc.,
Niantic, Inc., Pinterest, Inc.,
Reddit, Inc., Snap, Inc., and
Twitter Inc.

Dated: December 30, 2016

APPLE INC.

By: Jeffrey Landis
Jeffrey Landis
ZwillGen PLLC
1900 M Street NW, Suite 250
Washington, DC 20036
jeff@zwillgen.com
202-706-5203
Counsel for Proposed *Amicus*
Curiae Apple Inc.

Dated: December 30, 2016

RED HAT INC.

By: _____
David B. Perry
100 East Davie Street
Raleigh, NC 27601
dperry@redhat.com
Counsel for Proposed *Amicus*
Curiae Red Hat Inc.

Dated: December 30, 2016

PERKINS COIE LLP

Of Counsel:

Eric D. Miller*

Todd M. Hinnen*

Erin K. Earl*

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

By: _____

Jeffrey D. Vanacore
30 Rockefeller Plaza
New York, New York 10112
Tel.: (212) 262-6900
Fax: (212) 399-8021
jvanacore@perkinscoie.com

Counsel for Proposed *Amici Curiae* Amazon.com, Inc., Box, Inc., Dropbox Inc., Google Inc., Microsoft Corporation, Mozilla Corporation, Nest Labs, Inc., Niantic, Inc., Pinterest, Inc., Reddit, Inc., Snap, Inc., and Twitter Inc.

Dated: December 30, 2016

APPLE INC.

By: _____

Jeffrey Landis
ZwillGen PLLC
1900 M Street NW, Suite 250
Washington, DC 20036
jeff@zwillgen.com
202-706-5203

Counsel for Proposed *Amicus Curiae* Apple Inc.

Dated: December 30, 2016

RED HAT INC

By: _____

David B. Perry
100 East Davie Street
Raleigh, NC 27601
dperry@redhat.com

Counsel for Proposed *Amicus Curiae* Red Hat Inc.

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.
Gabriel K. Gillett
Gibson, Dunn & Crutcher LLP
200 Park Avenue
New York, NY 10166-0193
Counsel for Appellants

Exhibit A

Court of Appeals of the State of New York

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

FACEBOOK, INC.,

Appellant,

– against –

NEW YORK COUNTY DISTRICT ATTORNEY'S OFFICE,

Respondent.

IN THE MATTER OF THE MOTION TO COMPEL DISCLOSURE OF THE SUPPORTING
AFFIDAVIT RELATING TO CERTAIN SEARCH WARRANTS DIRECTED TO
FACEBOOK, INC., DATED JULY 23, 2013

FACEBOOK, INC.,

Appellant,

– against –

NEW YORK COUNTY DISTRICT ATTORNEY'S OFFICE,

Respondent.

**BRIEF OF AMAZON.COM, INC., APPLE INC., BOX, INC., DROPBOX INC.,
GOOGLE INC., MICROSOFT CORPORATION, MOZILLA CORPORATION,
NEST LABS, INC., NIANTIC, INC., PINTEREST, INC., RED HAT INC.,
REDDIT, INC., SNAP INC., AND TWITTER INC. AS *AMICI CURIAE* IN
SUPPORT OF APPELLANT**

JEFFREY LANDIS
ZwillGen PLLC
1900 M Street NW, Suite 250
Washington, DC 20036
Counsel for Apple Inc.

DAVID B. PERRY
RED HAT INC.
100 East Davie Street
Raleigh, NC 27601
Counsel for Red Hat Inc.

JEFFREY D. VANACORE
Counsel of Record
ERIC D. MILLER
TODD M. HINNEN
ERIN K. EARL
PERKINS COIE LLP
30 Rockefeller Plaza
New York, New York 10112
Tel.: (212) 262-6900
Fax: (212) 399-8021
*Counsel for Amazon.com, Inc.,
Box, Inc., Dropbox Inc.,
Google Inc., Microsoft
Corporation, Mozilla
Corporation, Nest Labs
Inc., Niantic, Inc.,
Pinterest, Inc., Reddit, Inc.,
Snap Inc., and Twitter Inc.*

TABLE OF CONTENTS

	Page
STATEMENT OF INTEREST OF <i>AMICI CURIAE</i>	1
SUMMARY OF THE ARGUMENT	5
ARGUMENT	7
I. A third-party provider must be able to challenge a warrant that the provider is charged with executing on behalf of law enforcement.....	8
A. This case involves a warrant executed by a communications service provider, not by a government official.....	9
B. The Fourth Amendment requires that the person executing a warrant assess its validity and challenge it if it appears invalid.....	11
C. Because the SCA prohibits providers from knowingly complying with facially invalid warrants, it contemplates that providers will be able to challenge them.....	14
D. Additional safeguards are critical to protect Fourth Amendment interests in the context of SCA warrants.	17
II. By characterizing Facebook’s appeal as taken from a nonappealable order, the First Department misapplied the law and created a rule that deprives the public of appellate guidance on issues of national import.	21
III. The lower court’s decision let stand an unconstitutional warrant accompanied by a gag order that violates federal statutory law and the First Amendment.....	24
A. The gag order is an unconstitutional prior restraint.....	25
B. The gag order cannot satisfy strict scrutiny.....	26
C. If the Court construes the SCA to avoid the First Amendment issue, the gag order violates the SCA itself.	28
CONCLUSION	30

TABLE OF AUTHORITIES

	Page(s)
CASES	
<i>Alexander v. United States</i> , 509 U.S. 544 (1993)	25
<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)	10
<i>Bantam Books, Inc. v. Sullivan</i> , 372 U.S. 58 (1963)	25
<i>Bivens v. Six Unknown Named Agents of the Fed. Bureau of Narcotics</i> , 403 U.S. 388 (1971)	11
<i>Brown v. Entm't Merchs. Ass'n</i> , 564 U.S. 786 (2011)	26
<i>Brown v. Illinois</i> , 422 U.S. 590 (1975)	12
<i>Freedman v. Am. Online, Inc.</i> , 325 F. Supp. 2d 638 (E.D. Va. 2004)	14
<i>Frisby v. Schultz</i> , 487 U.S. 474 (1988)	27
<i>Groh v. Ramirez</i> , 540 U.S. 551 (2004)	11
<i>In re 381 Search Warrants Directed to Facebook, Inc.</i> , 14 N.Y.S.3d 23, 132 A.D.3d 11 (N.Y. App. Div. 2015)	16
<i>In re Grand Jury Subpoena for: [Redacted]@yahoo.com</i> , 79 F. Supp. 3d 1091 (N.D. Cal. 2015)	29
<i>In re Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders</i> , 562 F. Supp. 2d 876 (S.D. Tex. 2008)	29

<i>In re Search of Elec. Commc 'ns in the Account of chakafattah@gmail.com at Internet Serv. Provider Google, Inc., 802 F.3d 516 (3d Cir. Sept. 2, 2015)</i>	20
<i>In re Search Warrant, 193 Vt. 51, 71 A.3d 1158 (2012)</i>	10
<i>In re Search Warrant for [Redacted]@hotmail.com, 74 F. Supp. 3d 1184, 1185 (N.D. Cal. 2014)</i>	29
<i>In re Search Warrants Directed to Facebook, 132 A.D.3d 11, 14 N.Y.S.3d 23 (1st Dept. 2015)</i>	8, 11, 22, 23
<i>In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014), aff'd, No. 13-mj-02814, ECF No. 80 (S.D.N.Y. Aug. 11, 2014)</i>	20
<i>In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016)</i>	20
<i>Landmark Commc 'ns, Inc. v. Virginia, 435 U.S. 829 (1978)</i>	28
<i>Malley v. Briggs, 475 U.S. 335 (1986)</i>	11
<i>Messerschmidt v. Millender, 132 S. Ct. 1235 (2012)</i>	11, 12
<i>Mills v. Alabama, 384 U.S. 214 (1966)</i>	28
<i>N.Y. Times Co. v. United States, 403 U.S. 713 (1971)</i>	26
<i>NAACP v. Button, 371 U.S. 415 (1963)</i>	27
<i>Near v. Minnesota ex rel. Olson, 283 U.S. 697 (1931)</i>	25

<i>People v. Bautista</i> , 7 N.Y.3d 838 (2006)	22
<i>People v. Marin</i> , 86 A.D.2d 40, 448 N.Y.S.2d 748 (1982)	22
<i>R.A.V. v. City of St. Paul</i> , 505 U.S. 377 (1992)	28
<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)	12
<i>Reno v. ACLU</i> , 521 U.S. 844 (1997)	26, 27
<i>United States v. Brooks</i> , 427 F.3d 1246 (10th Cir. 2005)	13
<i>United States v. Graziano</i> , 558 F. Supp. 2d 304 (E.D.N.Y. 2008)	13
<i>United States v. Leon</i> , 468 U.S. 897 (1984)	12
<i>United States v. Playboy Entm't Grp., Inc.</i> , 529 U.S. 803 (2000)	26
<i>United States v. Ryan</i> , 402 U.S. 530 (1971)	16
<i>United States v. Spencer</i> , 530 F.3d 1003 (D.C. Cir. 2008)	12

STATUTES

18 U.S.C. § 2702(a)	14
18 U.S.C. § 2702(a)(3)	9
18 U.S.C. § 2702(b)	14
18 U.S.C. § 2703	9

18 U.S.C. § 2703(a).....	9, 17
18 U.S.C. §2703(d).....	16, 17
18 U.S.C. § 2703(e).....	15
18 U.S.C. § 2703(g).....	10
18 U.S.C. § 2705(b).....	28, 29
18 U.S.C. § 2707	14
18 U.S.C. § 2707(e).....	15
18 U.S.C. § 3105	9
42 U.S.C. § 1983	11
N.Y. Crim. Proc. Law § 690.05(2).....	9
N.Y. Crim. Proc. Law § 690.10.....	9
N.Y. Crim. Proc. Law § 690.25(1).....	9
Stored Communications Act, 18 U.S.C. §§ 2701-2712	passim

OTHER AUTHORITIES

Fed. R. Crim. P. 41	9
Paul K. Ohm, <i>Parallel-Effect Statutes and E-Mail “Warrants”: Reframing the Internet Surveillance Debate</i> , 72 Geo. Wash. L. Rev. 1599 (2004).....	10
Paul Ohm, <i>Massive Hard Drives, General Warrants, and the Power of Magistrate Judges</i> , 97 Va. L. Rev. Online (2011).....	18
U.S. Const. amend. I.....	passim
U.S. Const. amend. IV.....	passim

STATEMENT OF INTEREST OF *AMICI CURIAE*

Amazon.com, Inc., based in Seattle, Washington, is one of the world's largest and best known online retailers and cloud service providers. Amazon seeks to be the Earth's most customer-centric company, where customers can discover anything they might want to buy online at the lowest possible prices. Amazon's cloud computing business, Amazon Web Services, is trusted by more than a million active customers around the world—including the fastest growing startups, largest enterprises, and leading government agencies—to power their IT infrastructure, make them more agile, and lower costs.

Apple Inc. revolutionized personal technology with the introduction of the Macintosh in 1984. Today, Apple leads the world in innovation with iPhone, iPad, Mac, Apple Watch, and Apple TV. Apple's four software platforms—iOS, macOS, watchOS, and tvOS—provide seamless experiences across all Apple devices and empower people with breakthrough services including the App Store, Apple Music, Apple Pay and iCloud. Apple's more than 100,000 employees are dedicated to making the best products on earth, and to leaving the world better than we found it.

Box, Inc. is a cloud-based enterprise content management platform that makes it easier for people to securely collaborate and get work done faster. Today, more than 41 million users and over 66,000 businesses—including 60% of the Fortune 500—trust Box to manage content in the cloud.

Dropbox Inc. provides file storage, synchronization, and collaboration services. With over 500 million users and 200,000 businesses, people around the world use Dropbox to work the way they want, on any device, wherever they go. Dropbox's products are built on trust; when people put their files in Dropbox, they can trust they're secure and their data is their own.

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 leader in the technology industry. Since its founding in 1975, it has developed a wide range of software, services, and hardware products, including the flagship Windows operating system, the Office suite of productivity applications, the Surface tablet computer, and the Xbox gaming system.

Mozilla Corporation is a global, mission-driven organization that works with a worldwide community to create open source products like its web browser Firefox. Its mission is guided by the Mozilla Manifesto, a set of principles that recognizes, among other things, that individuals' security and privacy on the Internet are fundamental and must not be treated as optional. In furtherance of that,

Mozilla has also adopted data-privacy principles that emphasize transparency, user control, limited data collection, and multi-layered security control and practices.

Nest Labs Inc., builds hardware, software, and services for the connected home. Nest algorithms use data about customer's preferences to adapt and optimize device behavior.

Niantic, Inc. is a developer and publisher of location-based, augmented reality mobile applications, including Pokémon GO, Ingress, and Field Trip, that are designed to engage players with their real world surroundings and to encourage them to explore unique and interesting aspects of their local communities and places they visit. Niantic's applications have been downloaded and used by hundreds of millions of people around the world. Due to the widespread use of its products, Niantic regularly receives law enforcement data requests similar to those at issue in this appeal. Niantic is based in San Francisco, California.

Pinterest, Inc. provides an online catalog of ideas. Every month, over 150 million people around the world use Pinterest to find and save ideas for cooking, parenting, style, and more.

Red Hat Inc. is the world's leading provider of open source software to enterprise customers, using a community-powered approach to develop and offer reliable and high-performing operating system, virtualization, management, middleware, cloud, mobile and storage technologies. Its software products are used

by Wall Street investment firms, hundreds of Fortune 500 companies, and the United States government. Based in Raleigh, North Carolina, Red Hat has offices in 33 countries.

Reddit, Inc. operates the reddit.com platform, which is a collection of thousands of online communities attracting over 260 million monthly unique visitors that create, read, join, discuss, and vote on conversations across a myriad of topics. Reddit is based in San Francisco, CA.

Snap Inc. is a camera company whose products empower people to express themselves, live in the moment, learn about the world, and have fun together. Snap Inc.'s first product, Snapchat, is one of the world's leading camera applications. Because more than 150 million people use Snapchat each day to capture images and send messages, Snap Inc. regularly receives law enforcement data requests governed by the statutory framework at issue in this case.

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.

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* regularly receive

search warrants and related legal requests from federal, state, and local law enforcement. Because *amici* are committed to user privacy, they scrutinize such legal process 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* object to the legal process or seek to have law enforcement 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 such requests providers receive, some of the *amici* publish regular transparency reports containing aggregate information about these requests.

Some *amici* have challenged warrants in court before. Although many such challenges are brought under seal and 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. Courts have also entertained appeals of those orders. *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 this case.

SUMMARY OF THE ARGUMENT

Amici support Facebook in this appeal because they share Facebook's views on the critical and recurring questions of law presented in this case, which will

affect the lives of individuals across New York and the United States. *Amici* focus on three issues of particular importance under the Stored Communications Act (“SCA”), 18 U.S.C. §§ 2701-2712.

First, the lower court erred in reaching the novel conclusion that there is no right to challenge an allegedly defective warrant before it is executed. 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. A pre-execution right of 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, if a provider can seek review of an allegedly defective SCA warrant, it also can appeal an order denying it relief. In deciding otherwise, the lower court ignored the unique posture of providers like Facebook and *amici*, who execute warrants under the SCA but who cannot seek review from a final judgment in the underlying criminal proceeding. Appellate review in these circumstances is necessary to provide full relief to providers.

Third, the gag order that accompanied the warrant violates the First Amendment, which requires that any content-based restriction on speech be narrowly tailored to serve a compelling government interest. Such a disclosure prohibition, which contains no time limit, is the antithesis of narrow tailoring. The Court may be able to construe the SCA to forbid such gag orders of infinite duration, thereby avoiding the constitutional issue. But if the SCA is so read, then the statute itself precludes the order here.

The combination of the lower court's Fourth Amendment theory and its First Amendment theory is particularly troubling.

Under the rule set forth by the First Department, a provider would have no recourse to question the validity of a warrant issued under the SCA, and could be forever precluded from speaking about it. Common sense dictates that service providers must be able to challenge invalid legal process directed to their users' information. Users trust services like Facebook's and *amici's* to safeguard their information. That trust is eroded by a rule stating that providers have no forum in which to challenge unlawful government demands for information.

ARGUMENT

The bulk warrants directed at Facebook sought the information of 381 individuals. But the rule established by the lower court offers no avenue for providers like Facebook and *amici* to even question whether such a warrant is constitutional. Thus, even if the warrant demanded content from 3,810

individuals—or 38,100 individuals—the provider executing the warrant would have no avenue to seek relief, on its own behalf or on behalf of its users, or to complain that a constitutional defect may be present. In fact, 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 unless the warrant bore fruit. In that case, the few individuals actually prosecuted for a crime could seek the suppression of evidence based on the warrant, but the innocent individuals swept up by the warrant would have no such remedy. This result is contrary to the law, and this Court should reject it.

I. A third-party provider must be able to challenge a warrant that the provider is charged with executing on behalf of law enforcement.

The First Department held that there is no constitutional or statutory right to challenge an allegedly defective warrant before it is executed. *In re Search Warrants Directed to Facebook*, 132 A.D.3d 11, 14 N.Y.S.3d 23 (1st Dept. 2015). Though this may be the well-settled rule for challenges to physical search warrants, this Court has never considered whether this is the correct rule to apply to warrants for electronic communications issued under the Stored Communications Act, 18 U.S.C. §§ 2701-2712 (the “SCA”). It is not. Because providers execute SCA warrants on behalf of law enforcement, they are legally

entitled to a pre-execution right of review, under both the Fourth Amendment and the SCA.

A. This case involves a warrant executed by a communications service provider, not by a government official.

The warrants in this litigation are governed by the SCA. *See* A5 (trial court order relying on the SCA as 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).

Ordinarily, a warrant authorizing a physical search is served and executed by an officer 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. 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.

In contrast, when a warrant is served on an online provider under the SCA, the provider is expected to fulfill its obligations, 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 by 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., 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). 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 First Department assessed that it made no difference to the outcome of the appeal that the SCA charged Facebook with executing the warrant on behalf of the government. 132 A.D.3d at 19. That is incorrect.

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). The presence of a warrant, however, “does not end the inquiry into objective reasonableness.” *Id.* Instead, 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 . . . that the executing officers cannot reasonably presume it to be valid.” *United States v. Leon*, 468 U.S. 897, 923 (1984) (quoting *Brown v. Illinois*, 422 U.S. 590, 610-11 (1975) (Powell, J., concurring in part)); accord *Messerschmidt*, 132 S. Ct. at 1245.

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 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 officer lacked qualified immunity for executing 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).

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 due to the potential for ambiguity in specifying how the search is to be conducted. 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. 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 different types of 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 does not exist or cannot be obtained using a provider’s existing systems or capabilities. Where a

provider is unable to reach a resolution 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 states and 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”). 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. Because the SCA prohibits providers from knowingly complying with facially invalid warrants, it contemplates that providers will be able to challenge them.

The SCA 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.

The SCA contains two provisions immunizing providers from liability for complying with a warrant. 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). 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 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 decision below, 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; 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.

Indeed, SCA Section 2703(d) grants online providers standing to move to quash warrants issued under the Stored Communications Act. The First Department determined, as a matter of first impression, that “2703(d), which gives the ISP the right to object, applies only to court orders or subpoenas issued under subsections (b) or (c)” and not “warrants, which are governed by . . . subsection (a).” *In re 381 Search Warrants Directed to Facebook, Inc.*, 14 N.Y.S.3d 23, 29, 132 A.D.3d 11 (N.Y. App. Div. 2015). This interpretation is incorrect. It is true that the first sentence of 2703(d) refers only to court orders issued under subsections (b) and (c). But the second sentence of Section 2703(d) grants a right to providers to move to quash or modify any order issued “pursuant to this section.” Had Congress intended to limit a provider’s pre-execution right of review

to court orders issued under subsections (b) and (c), it would have said so. Instead, the statute permits a motion to quash or modify any order issued “pursuant to this section.” “This” section is Section 2703, and SCA warrants are issued under Section 2703(a). Accordingly, the pre-execution right of review extends to SCA warrants.

Further, though Section 2703(d) specifically mentions objections related to voluminous records and undue burden, the provision does not mean that providers cannot challenge a warrant on the ground that it is ambiguous, invalid, or illegal. To the contrary, because compliance with a facially invalid warrant could 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 a pre-execution right of review.

Finally, even if Section 2703(d) were more limited, there is nothing within the SCA that forecloses a provider from challenging an SCA warrant in court before executing it. Rather, the immunity provisions clearly contemplate that providers would have such a right in the ordinary course.

D. Additional safeguards are critical to protect Fourth Amendment interests in the context of SCA warrants.

The system for which the government advocates is one in which providers would receive secret SCA warrants from law enforcement requiring providers to

collect and disclose information about their users, and the providers would blindly fill them. Under this system, it would not matter how much information was sought, how many users the warrant covered, or even whether the warrant had been signed by a judge or otherwise bore indicia of validity.

Both the government and the First Department point to safeguards that allegedly protect against abuses, but they ignore the realities of SCA warrants and, in doing so, they ignore the safeguards' ineffectiveness in this context. First, while pre-execution review for probable cause supporting SCA warrants is required under the SCA and is critical to provide a baseline of legitimacy, it is not sufficient to protect Fourth Amendment interests in the context of search warrants for electronic information stored in evolving third party platforms. When considering an SCA warrant, magistrates may not even know when a warrant is unconstitutional because—having before them only the government's ex parte presentation—they may not sufficiently understand the technology to assess whether the scope of information being sought is tailored to the crime under investigation. *See Paul Ohm, Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 Va. L. Rev. In Brief 1, 5 (2011) (noting that “[i]n the pre-computer age, judges allowed some forms of over collection as a constitutional compromise . . . [and] let the police haul entire filing cabinets containing evidence commingled with innocent material back to the station” but

that in today's high-tech world, "we must ask whether the filing cabinet solution continues to strike the proper balance"). Permitting a neutral third party like Facebook to explain to the court how the relevant systems work, what type of data is covered by the warrant, and why the warrant may not survive constitutional scrutiny in the context of its particular platform can be critically important to a magistrate tasked with protecting Fourth Amendment interests.

Second, ex post review is unsatisfactory because it generally requires a prosecution. For providers and other innocent parties to a massive set of warrants like those at issue here, there is little solace in the possibility that an alleged criminal involved in the same investigation may find it expedient to challenge the warrants covering the same information. In this case, hundreds of the individuals subject to the bulk warrants were not prosecuted and, had the court not lifted the perpetual nondisclosure order that issued with the warrants, they would never even have known that they had a right to vindicate. Providers are left with no remedy. Though Facebook spent valuable resources filling hundreds of broad-ranging warrants and risked jeopardizing the trust of its users in doing so, the government contends that it is powerless to seek judicial redress.

The Fourth Amendment safeguards that apply to physical search warrants are insufficient in the context of SCA warrants. The interests of law enforcement, while great, do not justify adhering to traditional practices and refusing to employ

the common-sense measures contemplated by the SCA. Indeed, throughout this case, the government has cited to no specific harm resulting from Facebook's attempt to seek review of the bulk warrants.

Other courts have entertained challenges to SCA warrants. The U.S. Court of Appeals for the Second Circuit recently reviewed the denial of a service provider's motion to quash an SCA warrant. *See In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.* ("Microsoft"), 829 F.3d 197, 201-02 (2d Cir. 2016). At no point did the court question the provider's right to challenge the warrant through a pre-execution motion to quash—which also had been implicitly recognized by the Magistrate Judge and District Judge below. *See In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 15 F. Supp. 3d 466, 471-72, 474 n.4 (S.D.N.Y. 2014), *aff'd*, No. 13-mj-02814, ECF No. 80 (S.D.N.Y. Aug. 11, 2014). Instead, the court considered the merits of the parties' arguments, held "that the District Court lacked the authority to enforce the Warrant against" the provider, and remanded with instructions to quash the contested portions of the warrant. *Microsoft*, 829 F.3d at 201-02; *see also, e.g., In re Search of Elec. Commc'ns in the Account of chakafattah@gmail.com at Internet Serv. Provider Google, Inc.*, 802 F.3d 516, 521 (3d Cir. Sept. 2, 2015). This Court should do the same.

II. By characterizing Facebook’s appeal as taken from a nonappealable order, the First Department misapplied the law and created a rule that deprives the public of appellate guidance on issues of national import.

The First Department improperly dismissed Facebook’s appeal as taken from nonappealable orders. Like the ruling regarding a provider’s right to challenge an SCA warrant, the ruling on appealability ignores the distinction between traditional search warrants and those issued under the SCA, which, as explained above, are executed by third-party providers. While the government frames the issue as one that has been litigated time and again, no New York court has ever addressed whether an appeal may be taken from an order seeking to quash an SCA warrant. The rule announced by the First Department deprives providers like Facebook and *amici* of the opportunity to vindicate their rights before an appellate body. Just as importantly, it deprives parties and judges of meaningful guidance from appellate courts concerning the critical issues at the intersection of the Fourth Amendment and the SCA. This Court should clarify that limitations on appeals from criminal cases do not apply to appeals from motions to quash allegedly defective SCA warrants. New York law recognizes that unique circumstances arising from third-party involvement in criminal proceedings warrant an exception to the rule against appeals from interlocutory orders in criminal actions.

Below, the First Department cited the rule that “[d]irect appellate review of interlocutory orders issued in a criminal proceedings is not available absent

statutory authority.” 132 A.D.3d at 18 (citing *People v. Bautista*, 7 N.Y.3d 838 (2006)). New York courts have recognized, however, that an exception applies when the interlocutory order affects a third party to the criminal action. *See People v. Marin*, 86 A.D.2d 40, 42, 448 N.Y.S.2d 748 (1982).

In *Marin*, a criminal defendant subpoenaed documents from a third party in connection with a criminal trial. *Id.* at 42-43. The third-party law firm moved to quash the subpoena and obtained partial relief. *Id.* On appeal, the criminal defendant argued that no appeal lies from an interlocutory order in a criminal action. *Id.* at 43. The Court disagreed, noting that while no appeal may lie from an order involving a *party* to the criminal action, this rule is premised on the fact that “the propriety of such an order can be resolved on the direct appeal from any resulting judgment of conviction.” *Id.* In the case of third parties, the Court noted that this “avenue of relief is totally unavailable,” and “the denial of an appeal to the law firm at this juncture would irrevocably preclude it from any opportunity to vindicate its position before an appellate body.” *Id.* It held that the motion to quash was final and appealable as to the third-party law firm.

The same rationale applies here. Facebook cannot appeal from a final judgment entered against one of the individuals about which it was compelled to produce information. Accordingly, the justifications for limiting an appeal from an interlocutory criminal order simply do not exist as applied to a third party like

Facebook. And there is no logical reason offered by the lower court or the government for distinguishing an order to quash a subpoena from an order to quash a warrant for purposes of establishing appealability. The dearth of authority concerning the appealability of motions to quash warrants, as opposed to subpoenas, reflects that such motions are unique to the SCA, as set forth above in Section I.

The interests at stake when law enforcement attempts to surreptitiously gain access to individuals' private communications compel appellate courts to provide meaningful guidance to judges, providers, and individuals alike. Yet the result of the First Department's order is a system whereby trial court judges and magistrates, who have "the power to affect the everyday lives of all U.S. residents," *In re Search Warrants Directed to Facebook*, 132 A.D.3d at 22-23, are never provided more than one side of the story and only rarely will have the benefit or an even partial analysis of the issues by the higher courts.

The First Department's order describes the "indispensable responsibility" assigned to judges and magistrates that review warrant applications. *Id.* at 23. It also provides lengthy instructions about the standards that a judge should apply when reviewing a warrant request. *Id.* at 24. Ironically, the First Department's own guidance on this topic could not have been offered had Facebook not sought to appeal the trial court's order in this case. Thus, the lower court's own order

confirms the need for appellate review of orders challenging warrants under the SCA.

III. The lower court's decision let stand an unconstitutional warrant accompanied by a gag order that violates federal statutory law and the First Amendment.

This Court should also reverse the trial court's approval of an unconstitutional bulk warrant accompanied by an unconstitutional gag order and the trial court's refusal to compel the government to disclose the affidavit underlying its criminal investigation. Although the government argues that many of these issues are either moot or imperfectly preserved, *amici* agree with Facebook that these important questions of law are properly before this Court. *See* Reply Br. of Appellant, at 23-25, 32, 35.

Facebook has addressed the Fourth Amendment issues attendant to the bulk warrants that instigated this dispute, and *amici* share those views. Facebook correctly argues that the warrants in this case were overbroad in that they sought all of hundreds of users' account information, including vast stores of information, much of which could have no conceivable relevance to the crimes under investigation. Appellant's Opening Br. at 37-46. Further, although the case is now unsealed, the government refuses to release the affidavit, supporting an inference that it not only was overbroad but also lacked sufficient probable cause for so many accounts.

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 the First Amendment and cannot be enforced. And if the Court reads the SCA to forbid indefinite gag orders, thus avoiding the constitutional issue, the statute itself bars the nondisclosure order here.

A. The gag order is an unconstitutional prior restraint.

The gag order violates 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).

B. 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*, 564 U.S. 786, 799 (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 be such a reason in this case, the trial court failed to articulate it.

But even assuming 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 the Government alleges might result from the disclosure of the affidavit now, that harm is highly unlikely because the existence of the investigation has been revealed, the Government has obtained the few indictments it sought, and the investigation is over. 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); *accord Landmark Commc'ns, Inc. v. Virginia*, 435 U.S. 829, 838 (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).

C. If the Court construes the SCA to avoid the First Amendment issue, the gag order violates the SCA itself.

Courts commonly construe statutes to avoid constitutional issues. Here, the Court may be able to construe the SCA to require the sort of careful tailoring the First Amendment demands. But in that event, the gag order falls short of the statutory requirement, given the manifest failure to limit the order to avoid treading on important First Amendment interests.

Under 18 U.S.C. § 2705(b), a court may forbid an electronic communications service provider from giving 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” could be read to mean that such an order must last only for a limited time, consistent with the First Amendment. *See In re Search Warrant for [Redacted]@hotmail.com* (“Hotmail”), 74 F. Supp. 3d 1184, 1185 (N.D. Cal. 2014); *accord In re Grand Jury Subpoena for: [Redacted]@yahoo.com*, 79 F. Supp. 3d 1091, 1093 (N.D. Cal. 2015).

But even without that limitation, the five enumerated factors, all of which are tied to an ongoing investigation, compel the conclusion that the order here falls short. 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 here articulated no reason to think that such harms could result. Accordingly, to the extent the SCA is read to pass constitutional muster, the permanent gag order violates the SCA. *See, e.g., Hotmail*, 74 F. Supp. 3d at 1186 (“A limited period of nondisclosure, as justified by the government’s initial application, coupled with an obligation on the government to seek renewal if the circumstances justifying the initial period remain in effect, better squares with Section 2705(b)’s language and purpose.”); *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.”).

CONCLUSION

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

Respectfully submitted

Of Counsel:
Eric D. Miller*
Todd M. Hinnen*
Erin K. Earl*

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

PERKINS COIE LLP

By: Jeffrey D. Vanacore/TMH
Jeffrey D. Vanacore
30 Rockefeller Plaza
New York, New York 10112
Tel.: (212) 262-6900
Fax: (212) 399-8021
jvanacore@perkinscoie.com

Counsel for *Amici Curiae* Amazon.com, Inc., Box, Inc., Dropbox Inc., Google Inc., Microsoft Corporation, Mozilla Corporation, Nest Labs, Inc., Niantic, Inc., Pinterest, Inc., Reddit, Inc., Snap, Inc., and Twitter Inc.

APPLE INC.

By: Jeffrey Landis
Jeffrey Landis
ZwillGen PLLC
1900 M Street NW, Suite 250
Washington, DC 20036
jeff@zwillgen.com
202-706-5203

Counsel for *Amicus Curiae* Apple Inc.

RED HAT INC.

By:

David B. Perry
David B. Perry
100 East Davie Street
Raleigh, NC 27601
dperry@redhat.com

Counsel for *Amicus Curiae*
Red Hat Inc.

Respectfully submitted

Of Counsel:

Eric D. Miller*

Todd M. Hinnen*

Erin K. Earl*

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

PERKINS COIE LLP

By: _____

Jeffrey D. Vanacore
30 Rockefeller Plaza
New York, New York 10112
Tel.: (212) 262-6900
Fax: (212) 399-8021
jvanacore@perkinscoie.com

Counsel for *Amici Curiae* Amazon.com, Inc., Box, Inc., Dropbox Inc., Google Inc., Microsoft Corporation, Mozilla Corporation, Nest Labs, Inc., Niantic, Inc., Pinterest, Inc., Reddit, Inc., Snap, Inc., and Twitter Inc.

APPLE INC.

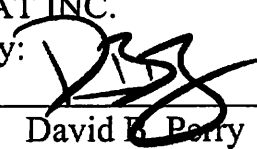
By: _____

Jeffrey Landis
ZwillGen PLLC
1900 M Street NW, Suite 250
Washington, DC 20036
jeff@zwillgen.com
202-706-5203

Counsel for *Amicus Curiae* Apple Inc.

RED HAT INC.

By: _____


David K. Perry
100 East Davie Street
Raleigh, NC 27601
dperry@redhat.com

Counsel for *Amicus Curiae*
Red Hat Inc.