
**New York State Supreme Court
Appellate Division – First Department**

Supreme Court Index No. 30207-13

FILED UNDER SEAL

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

OPENING BRIEF OF APPELLANT FACEBOOK, INC.

GIBSON, DUNN & CRUTCHER LLP
Orin Snyder
Alexander H. Southwell
Thomas H. Dupree, Jr. (*pro hac vice* pending)
Jane Kim
200 Park Avenue
New York, New York 10166
Telephone: (212) 351-4000
Fax: (212) 351-4035
jkim@gibsondunn.com

Attorneys for Appellant Facebook, Inc.

Dated: June 20, 2014

PRINTED ON RECYCLED PAPER

TABLE OF CONTENTS

	<u>Page</u>
QUESTIONS PRESENTED.....	1
PRELIMINARY STATEMENT	3
STATEMENT OF THE CASE.....	9
A. Facebook	9
B. The Bulk Warrants	11
C. Proceedings Below.....	14
ARGUMENT	16
I. THIS APPEAL IS PROPERLY BEFORE THIS COURT.	16
A. The Trial Court’s Order Is Appealable.	16
B. Facebook Has Standing To Challenge The Warrants.	22
II. THE BULK WARRANTS ARE UNCONSTITUTIONAL.	26
A. The Warrants Violate The Fourth Amendment.	26
1. The Fourth Amendment’s Protections Apply With Particular Force In The Digital Age.	26
2. The Bulk Warrants Are Overbroad, Lack Particularity, And Authorize General Searches.....	30
B. The Bulk Warrants’ Indefinite Gag Provisions Violate The Stored Communications Act And The First Amendment.....	39
1. The Gag Provisions Violate The Stored Communications Act.	39
2. The Gag Provisions Violate The First Amendment.	41
CONCLUSION.....	44

TABLE OF AUTHORITIES

	<u>Page(s)</u>
Cases	
<i>ACLU v. Clapper</i> , 959 F. Supp. 2d 724 (S.D.N.Y. 2013)	44
<i>Arizona v. Gant</i> , 556 U.S. 332 (2009).....	27
<i>B. T. Prods., Inc. v. Barr</i> , 44 N.Y.2d 226 (1978).....	21
<i>Butterworth v. Smith</i> , 494 U.S. 624 (1990).....	43
<i>Camara v. Mun. Ct. of City & Cnty. of San Francisco</i> , 387 U.S. 523 (1967).....	27
<i>Clark v. Martinez</i> , 543 U.S. 371 (2005).....	41
<i>Groh v. Ramirez</i> , 540 U.S. 551 (2004).....	35
<i>In re Appeal of Application for Search Warrant</i> , 71 A.3d 1158 (Vt. 2012).....	29
<i>In re Sealing and Non-Disclosure of Pen/Trap/2703(D) Orders</i> , 562 F. Supp. 2d 876 (S.D. Tex. 2008).....	9, 42, 43
<i>In re Search Warrants for Information Associated with Target Email Address</i> , 2012 WL 4383917 (D. Kan. Sept. 21, 2012).....	33
<i>In re: [REDACTED]@gmail.com</i> , No. 5:14-mj-70655-PSG (N.D. Cal. May 9, 2014)	37
<i>In the Matter of Applications for Search Warrants for Information Associated with Target Email Accounts/Skype Accounts</i> , 2013 WL 4647554 (D. Kan. Aug. 27, 2013).....	28, 36

TABLE OF AUTHORITIES

	<u>Page(s)</u>
<i>In the Matter of the Search of Information Associated with [Redacted] That Is Stored at Premises Controlled by Yahoo! Inc.,</i> No. 13-MJ-728 (D.D.C. Sept. 25, 2013)	37
<i>In the Matter of the Search of Information Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.,</i> 2014 WL 1377793 (D.D.C. Apr. 7, 2014).....	34, 38
<i>In the Matter of the Search of Information Associated with the Account Identified by the Username Aaron.Alexis,</i> 2013 WL 7856600 (D.D.C. Nov. 26, 2013)	37, 38
<i>Maryland v. Garrison,</i> 480 U.S. 79 (1987).....	27, 28
<i>Matter of Abrams,</i> 62 N.Y.2d 183 (1984)	17, 18, 19
<i>Matter of Boikess v. Aspland,</i> 24 N.Y.2d 136 (1969).....	17
<i>Matter of Cunningham v. Nadjari,</i> 39 N.Y.2d 314 (1976)	17
<i>Matter of Grand Jury Subpoenas,</i> 72 N.Y.2d 307 (1988).....	21
<i>Nebraska Press Ass’n v. Stuart,</i> 427 U.S. 539 (1976).....	24
<i>New York Cnty. Lawyers’ Ass’n v. State of New York,</i> 294 A.D.2d 69 (1st Dep’t 2002)	24, 25
<i>Payton v. New York,</i> 445 U.S. 573 (1980).....	27

TABLE OF AUTHORITIES

	<u>Page(s)</u>
<i>People v. Bagley</i> , 720 N.Y.S.2d 454 (1st Dep’t 2001).....	20
<i>People v. Harris</i> , 949 N.Y.S.2d 590 (N.Y. Crim. Ct. 2012).....	23, 27
<i>People v. Marin</i> , 86 A.D.2d 40 (2d Dep’t 1982).....	6, 19, 20, 24
<i>People v. Purley</i> , 297 A.D.2d 499 (1st Dep’t 2002).....	16, 20
<i>Saratoga Cty. Chamber of Commerce v. Pataki</i> , 100 N.Y.2d 801 (2003).....	22
<i>Soc’y of Plastics Indus., Inc. v. Cnty. of Suffolk</i> , 77 N.Y.2d 761 (1991).....	22, 23
<i>United States v. Barthelman</i> , 2013 WL 3946084 (D. Kan. July 31, 2013).....	33
<i>United States v. Burgess</i> , 576 F.3d 1078 (10th Cir. 2009).....	31
<i>United States v. Cioffi</i> , 668 F. Supp. 2d 385 (E.D.N.Y. 2009).....	28
<i>United States v. Comprehensive Drug Testing, Inc.</i> , 621 F.3d 1162 (9th Cir. 2010).....	38
<i>United States v. Galpin</i> , 720 F.3d 436 (2d Cir. 2013).....	27, 28, 29, 30, 32
<i>United States v. Ganas</i> , 2014 WL 2722618 (2d Cir. June 17, 2014).....	30, 37
<i>United States v. George</i> , 975 F.2d 72 (2d Cir. 1992).....	31, 35

TABLE OF AUTHORITIES

	<u>Page(s)</u>
<i>United States v. Leary</i> , 846 F.2d 592 (10th Cir. 1988)	35
<i>United States v. Otero</i> , 563 F.3d 1127 (10th Cir. 2009)	4, 30
<i>United States v. Rosa</i> , 626 F.3d 56 (2d Cir. 2010)	34
<i>United States v. Zemlyansky</i> , 945 F. Supp. 2d 438 (S.D.N.Y. 2013)	31, 35

Constitutional Provisions

U.S. Const. amend. IV	27
-----------------------------	----

Statutes

18 U.S.C. § 2701 <i>et seq.</i>	6
18 U.S.C. § 2703(b)	14, 23, 40
18 U.S.C. § 2703(d)	7, 18, 23
18 U.S.C. § 2705(b)	8, 40, 41
N.Y. C.P.L. § 690.35	23
N.Y. C.P.L.R. § 5701(a)	6, 17
N.Y. Penal Law § 155.35	13
N.Y. Penal Law § 155.40	13
N.Y. Penal Law § 175.35	13

TABLE OF AUTHORITIES

Page(s)

Other Authorities

Orin S. Kerr, <i>Applying the Fourth Amendment to the Internet: A General Approach</i> , 62 Stan. L. Rev. 1005 (2010).....	34
Orin S. Kerr, <i>Searches and Seizures in a Digital World</i> , 119 Harv. L. Rev. 531 (2005).....	29
P. Ohm, Response, <i>Massive Hard Drives, General Warrants, and the Power of Magistrate Judges</i> , 97 Va. L. Rev. in Brief 1 (2011).....	29
S. Rep. No. 99-541 (1986).....	23
William K. Rashbaum and James C. McKinley, Jr., <i>Charges for 106 in Huge Fraud Over Disability</i> , The New York Times (Jan. 8, 2014)	16

QUESTIONS PRESENTED

At the District Attorney's request, the trial court issued bulk search warrants directing Facebook to produce virtually all records and communications for 381 Facebook accounts. The warrants also include provisions barring Facebook from disclosing the existence of the warrants. The trial court subsequently unsealed 79 of the 381 warrants following grand jury indictments of some of the targeted Facebook users, but the remaining 302 warrants remain sealed. This appeal, which arises from the trial court's denial of Facebook's motion to quash the warrants, presents the following questions:

1. Is the order denying the motion to quash appealable? The trial court did not address this question.
2. Does Facebook—the party that was forced to comply with the warrants and that remains subject to the gag provisions—have standing to challenge the warrants? The trial court answered No.
3. Do the warrants, which authorized the seizure of voluminous amounts of personal information and communications without any meaningful date restrictions, content limitations, apparent connection to the crimes under investigation, or procedures requiring the return of the seized information, violate the Fourth Amendment? The trial court answered No.

4. Do the gag provisions of the warrants, which bar Facebook from disclosing their existence to 302 targeted users, even after the Government's investigation has concluded, violate the Stored Communications Act and the First Amendment? The trial court answered No.

This is an appeal by Facebook, Inc. of a Decision and Order of the Honorable Melissa C. Jackson, dated September 17, 2013 (the “Order”), denying Facebook’s motion to quash 381 search warrants and requiring Facebook to locate and produce user information.

PRELIMINARY STATEMENT

This appeal arises from the largest set of search warrants that Facebook has ever received and presents important questions concerning the lawful limits on searches and seizures in the digital age. As part of an investigation into an alleged scheme to fraudulently obtain disability benefits, the New York County District Attorney directed sweeping warrants at Facebook, demanding that it collect and turn over virtually all communications, data, and information from 381 Facebook accounts, yet only 62 of the targeted Facebook users were charged with any crime. The warrants also contained broad gag provisions barring Facebook from informing its users what the Government was forcing it to do.

The trial court’s refusal to quash the bulk warrants was erroneous and should be reversed. The Fourth Amendment does not permit the Government to seize, examine, and keep indefinitely the private messages, photographs, videos, and other communications of nearly 400 people—the vast majority of whom will never know that the Government has obtained and continues to possess their personal information. Nor does the First Amendment permit the Government to forbid

Facebook from ever disclosing what it has been compelled to do—even after the Government has concluded its investigation.

This appeal presents critical and recurring questions of constitutional law. Courts across the country continue to recognize the novel questions and significant constitutional risks posed by electronic searches and seizures, as well as the particular need for Fourth Amendment protections in the digital age. *See, e.g., United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009).

This case, of course, concerns Facebook—an online social networking service with more than one billion users. Many of these users treat Facebook as a digital home where they share personal and private information. They use Facebook to share photographs, videos, and communications of a personal nature, and they control the audience with whom they share this information.

The Government’s bulk warrants, which demand “all” communications and information in 24 broad categories from the 381 targeted accounts, are the digital equivalent of seizing everything in someone’s home. Except here, it is not a single home but an entire neighborhood of nearly 400 homes. A9-10 (Search Warrant at 1-2).¹ The vast scope of the Government’s search and seizure here would be unthinkable in the physical world.

¹ Facebook’s Appendix, filed and served on June 20, 2014, is cited as “A.”

The warrants cover a cross-section of America: nearly 400 people, high schoolers to grandparents, from all over New York and across the United States. The warrants target electricians, school teachers, and members of our armed services. *See* A104 (10/2/2013 Eckenwiler Aff., Ex. 1 at 10). They contain no date-range limitations, no limitations on the content to be seized and examined by the Government, and no procedures for the return of the seized information. *See* A9-10 (Search Warrant at 1-2). They demand information that cannot possibly be relevant to the crimes the Government presumably continues to investigate. Indeed, the main Facebook-related evidence presented publicly by the Government about this matter consists of a handful of photographs of a fraction of the targets acting in ways that are allegedly inconsistent with their claimed disabilities. The Government's own investigation thus confirms that most of the Facebook user data seized by the Government is irrelevant to the charges alleged, and the search warrants are overbroad and constitutionally defective.

Facebook takes its compliance obligations very seriously. *See* Facebook, Government Requests Report, <https://govtrequests.facebook.com>. At the same time, Facebook is committed to protecting its users from overbroad and unlawful governmental requests for data. Here, the Government has gone beyond what the Constitution permits and refuses to narrow intrusive and overbroad requests for private information. Critical constitutional rights are at stake.

This Court should reject the Government’s sweeping approach to search and seizure and reverse the judgment below for the following reasons.

First, Facebook is challenging an appealable order. The denial of the motion to quash the warrants is a civil rather than criminal order, just as the denial of a motion to quash a subpoena is civil rather than criminal, even when the subpoena is issued as part of a criminal investigation. Indeed, an order to produce documents pursuant to the Stored Communications Act operates much like a subpoena duces tecum.² Thus, Facebook may appeal as of right under N.Y. C.P.L.R. § 5701(a). The order is appealable for another reason: a third party may appeal orders directing it to produce documents for use in a criminal proceeding; this is a well-settled exception to the general rule against interlocutory appeals in criminal proceedings. *See, e.g., People v. Marin*, 86 A.D.2d 40, 42 (2d Dep’t 1982) (allowing appeal by third party “who is clearly aggrieved” by an order to produce documents in a criminal trial, because denying an appeal “would irrevocably preclude it from any opportunity to vindicate its position before an appellate body” since the third party has no right to appeal the verdict in the criminal case).

² The Stored Communications Act, enacted in 1986 as Title II of the Electronic Communications Privacy Act, addresses the disclosure of stored wire and electronic communications held by third-party providers of electronic communication services. 18 U.S.C. § 2701 *et seq.*

Second, Facebook has standing to challenge the bulk warrants. The Stored Communications Act—which the trial court repeatedly cited as providing the requisite statutory authority for the warrants—expressly grants service providers like Facebook the right to move to quash warrants issued pursuant to the Act. *See* 18 U.S.C. § 2703(d). Facebook also has standing because it has plainly suffered injuries-in-fact: both from the burden of having to gather and produce the information demanded by the Government, as well as from the gag provisions that enjoin Facebook from speaking publicly about what has happened. Finally, Facebook has third-party standing to assert the constitutional rights of its users whose private information has been seized without notice and is being held by the Government. The vast majority of these people have not been charged by the Government; they are thus unaware of the existence of the bulk warrants, and they are unable to assert their own constitutional rights.

Third, the bulk warrants violate the Fourth Amendment because they are overbroad and lack particularity. The trial court erred in failing to follow the lead of other courts that have enforced specific limits on warrants seeking digital information, ensuring that they satisfy the particularity requirement and are narrowly tailored to avoid the seizure of personal information that has no connection to the alleged crime. The warrants in this case are identical in scope: they demand 24 broad categories of information—including “[a]ny and all

subscriber and account information” and “[a]ny public or private messages”—without any meaningful limitations on the content or date range of the information to be seized. A9-10 (Search Warrant at 1-2). The warrants fail to link the demanded information to the suspected criminal activity. Compounding the problem, the warrants do not contain any provisions requiring the Government to return or destroy personal information that has nothing to do with the crimes under investigation.

Fourth, the bulk warrants’ gag provisions—which extend indefinitely and possibly forever for the vast majority of the targeted users—exceed the trial court’s authority under the Stored Communications Act to issue nondisclosure orders of *limited* duration. *See* 18 U.S.C. § 2705(b). Indeed, once the investigation with respect to the remaining 302 targeted accounts is concluded and any resulting indictments are announced, there can be no possible justification for maintaining secrecy. Furthermore, because the gag provisions are an indefinite, content-based restriction on Facebook’s speech concerning a matter of great public interest, they violate the First Amendment. *See In re Sealing and Non-Disclosure of Pen/Trap/2703(D) Orders*, 562 F. Supp. 2d 876, 878 (S.D. Tex. 2008).

Because the Constitution does not permit the Government to seize and indefinitely retain such vast quantities of private information—most of which

cannot possibly be related to the crimes under investigation—the judgment below must be reversed.

STATEMENT OF THE CASE

A. Facebook

Facebook is a popular online social networking service. It is a free, Internet-based platform that allows its more than one billion users worldwide to communicate, share information with friends and family, engage with issues and groups, and express and develop their identities. Facebook, Newsroom, Company Info., <http://newsroom.fb.com/company-info>. People who use Facebook share their opinions, ideas, photos, and videos about their lives, as well as send direct messages to others. More than two-thirds of Facebook’s users check Facebook on a daily basis. *Id.*

People who choose to use Facebook begin by creating a profile page or “Timeline” that typically provides the user’s name, photo, and biographical information.³ The timeline function allows people to post photographs or other information from their childhood to the present, enabling their friends or relatives to see their family history and meaningful personal events in their life. A profile page or “Timeline” typically identifies other Facebook users whom the user has

³ The terms “Timeline,” “Friend,” and “Like,” among other terms mentioned in this brief, are explained on the Facebook Help Center, www.facebook.com/help.

identified as a “Friend,” along with a list of other Facebook “Pages” or things the User has “Liked.” It often identifies places the person has been and events they have attended, along with accompanying photographs or videos. And it identifies the Facebook “Groups” to which the user belongs. Groups are online communities that can be organized around hobbies, types of food, political views, favorite sports teams—anything in which two or more people might have a shared interest. The identities of individual Group members are often known only to the members of the Group.

People use Facebook to share information about themselves, much of it personal. This information often includes:

- The person’s age, religion, location, city of birth, educational affiliations, employment, family members, children, grandchildren, partner, friends, places visited, favorite music, favorite movies, favorite television shows, favorite books, favorite quotes, things “Liked,” events to attend, affiliated Groups, fitness, sexual orientation, relationship status, political views;
- The person’s thoughts about: religion, sexual orientation, relationship status, political views, future aspirations, values, ethics, ideology, current events, fashion, friends, public figures,

celebrity, lifestyle, celebrations, grief, frustrations, infidelity, social interactions, or intimate behavior;

- The person’s photographs and videos of: him- or herself, children/family, friends, third parties, ultrasounds, medical experiences, food, lifestyle, pets/animals, travel/vacations, celebrations, music, art, humor, entertainment;
- The person’s private hardships meant to be shared only with friends; and
- The person’s intimate diary entries, including reflections, criticisms, and stories about daily life.

Facebook users have the ability to control who sees their information. Some choose to make some of their content public; others choose to limit information to their Facebook “Friends”; and still others choose to limit information to a subset of their Friends. They may adjust and fine-tune the privacy designations with regard to particular content, so that a user may elect to make certain content available only to a narrow audience, or even solely to him- or herself (thus creating a private space for a person’s most intimate information).

B. The Bulk Warrants

On July 23, 2013, the Supreme Court for New York County issued 381 search warrants directing Facebook to produce virtually all Facebook records and

communications for 381 Facebook accounts. A12 (Search Warrant at 4). Apart from the Facebook account identifiers, these 381 search warrants are carbon copies, bereft of any differentiation. Each stock warrant “COMMAND[S]” Facebook to “retrieve, enter, examine, copy, analyze, and to search the TARGET FACEBOOK ACCOUNT” for all evidence and property described in 24 separate categories, including:

- “Any and all subscriber and account information and user contact information”;
- The user’s “account status history . . . historical login information, mini-feed, status update history, shares, notes, wall and timeline postings to the target account, wall and timeline postings made by the target account to other accounts, friend listing, including deleted or removed friends . . . networks, group listing, future and past events, and video listing”;
- “[A]ll undeleted or saved photos”;
- “Any and all associated ‘Groups’ information, including a list of all other users currently registered in any such groups”;
- Any “private messages”;
- “All notes written and published to the account”; and

–“All chat history, including but not limited to, the content of all chats and date and time information for all chats”

A9-10 (Search Warrant at 1-2). The warrants identify many more categories and items; the foregoing are just examples from the beginning of the Government’s long list.

The warrants state that there is “reasonable cause to believe” that the property to be searched and seized “constitutes evidence and tends to demonstrate that an offense was committed including, but not limited to: Grand Larceny in the Second Degree in violation of Penal Law § 155.40; Grand Larceny in the Third Degree in violation of Penal Law § 155.35; Offering a False Instrument for Filing in the First Degree in violation of Penal Law § 175.35; and Conspiring to commit such crimes in the County of New York and elsewhere.” A11 (Search Warrant at 3).

The warrants also contain a provision prohibiting Facebook from ever disclosing their existence to the targeted Facebook users: “[P]ursuant to 18 U.S.C. § 2703(b), this court orders Facebook not to notify or otherwise disclose the existence or execution of this warrant/order to any associated user/account holder, since such disclosure could cause individuals to flee, destroy evidence, or otherwise interfere with an ongoing criminal investigation.” A11-12 (Search Warrant at 3-4).

C. Proceedings Below

Facebook received the warrants on July 24, 2013. Upon reviewing the scope of the District Attorney’s demands, Facebook asked the Government to narrow its broad requests—or at least permit Facebook to notify the users in question to enable them to determine whether to object. A26 (9/22/2013 Eckenwiler Aff. ¶ 3). The Government refused.

On August 20, Facebook moved to quash the bulk warrants as overly broad and lacking in particularity. Facebook also challenged the nondisclosure provisions. The trial court denied the motion to quash on September 17, finding that Facebook lacked standing. A6 (Order at 3). The court also rejected Facebook’s overbreadth and particularity challenges, reasoning that “[i]n the course of a long-term criminal investigation, the relevance or irrelevance of items seized within the scope of a search warrant may be unclear.” A6 (Order at 3). Finally, the court dismissed Facebook’s challenge to the gag provision. The court stated that it had “clear . . . authority to order nondisclosure of a pending investigation or existence of a court order,” and directed that the gag order “remains in effect until the court orders otherwise.” A7-8 (Order at 4-5).

Facebook moved this Court for a stay pending appeal. The Court granted an interim stay on September 23, but denied a full stay on November 19. *See* A17 (Order, *In Re: Anonymous*, M-4853 (1st Dep’t Nov. 19, 2013)). At that point,

Facebook complied with the warrants while continuing to pursue its appeal to this Court.⁴

In separate indictments dated January 6 and February 25, 2014, the Government indicted 62 of the targeted Facebook users. The Government alleged that these individuals had each engaged in a scheme to fraudulently obtain disability benefits by claiming they suffered from a disability when they did not. The Government supported its case in part through photographs obtained from Facebook that showed some of the targeted users acting in ways inconsistent with their claimed disabilities. *See* William K. Rashbaum and James C. McKinley, Jr., *Charges for 106 in Huge Fraud Over Disability*, *The New York Times* (Jan. 8, 2014). At the Government's request, the trial court ordered the unsealing and disclosure of 79 of the 381 search warrants directed to Facebook—the warrants aimed at 62 of the individuals named in the indictment—while leaving the remaining 302 warrants sealed and subject to the perpetual gag provision. A20-24 (1/6/2014 and 5/2/2014 Orders).

⁴ Although the trial court had issued an order to show cause because Facebook had not immediately complied with the trial court's September 17, 2013 Order denying its motion to quash, Facebook explained to the trial court that it had obtained an interim stay from this Court. Once this Court dissolved the interim stay, Facebook complied and the Government sent the trial court a letter noting Facebook's "immediate[] and full[]" compliance with the bulk warrants and asking the trial court to withdraw the order to show cause. A18 (12/4/2013 Serino Letter at 1).

ARGUMENT

I. THIS APPEAL IS PROPERLY BEFORE THIS COURT.

The Government has lodged threshold objections to appealability and standing in an effort to prevent this Court from resolving the important constitutional issues presented by this appeal. Neither of the Government's arguments has merit.

A. The Trial Court's Order Is Appealable.

In opposing a stay, the Government insisted that the Order is not appealable. But that is wrong. The Order is appealable for at least two reasons.

1. The denial of the motion to quash is a civil rather than criminal order, in that "it in no way affects the criminal proceeding or judgment itself and is entirely collateral to and discrete from the criminal proceeding." *People v. Purley*, 297 A.D.2d 499, 501 (1st Dep't 2002). Indeed, the Government's investigation has continued independent of this proceeding and, to Facebook's knowledge, the Government has not commenced any criminal proceedings against 302 of the targeted Facebook users. Because the trial court's Order plainly "affects a substantial right" of Facebook, it is appealable under N.Y. C.P.L.R. § 5701(a).

The Court of Appeals confronted a similar situation in *Matter of Abrams*, 62 N.Y.2d 183 (1984). There, the court held that a trial court order denying a motion to quash an Attorney General subpoena in a criminal investigation was a final and appealable order. The court explained that rather than focus on labels, "we have

looked to the true nature of the proceeding and to the relief sought in order to determine whether the proceeding was criminal or civil.” *Id.* at 191. Thus, the court explained, it had repeatedly deemed the denial of a motion to quash an appealable order—even when the Government was demanding documents for purposes of an ongoing criminal investigation. *Id.*; *see also, e.g., Matter of Boikess v. Aspland*, 24 N.Y.2d 136, 138-39 (1969) (denial of a motion to quash subpoenas issued in furtherance of a criminal investigation into drug abuse is a final and appealable order); *Matter of Cunningham v. Nadjari*, 39 N.Y.2d 314, 317 (1976) (recognizing “the direct appealability of orders granting or denying motions to quash subpoenas in criminal investigations”).

The Government has attempted to distinguish these cases by arguing that the order in this case arose from a motion to quash a search warrant, rather than a motion to quash a subpoena. But that label-based argument is directly contrary to the Court of Appeals’ holding in *Abrams*, where it emphasized that “we look to the nature of the proceeding and the relief sought” rather than whether the order arose in the context of a criminal investigation. 62 N.Y.2d at 193. Indeed, the *Abrams* court added that “we recognize that *at some time in the future* the Attorney General *may* file criminal charges . . . and thereby arguably commence a criminal proceeding,” but that where “the only aspect of the subject proceeding that is criminal in nature is the Attorney General’s investigation,” which may never result

in criminal charges, the proceeding is civil in nature. *Id.* (emphases in original).

The same rationale applies here.

This conclusion is reinforced by the fact that an order to produce electronic documents pursuant to the Stored Communications Act is very *similar* to a subpoena duces tecum—and very *dissimilar* to an ordinary search warrant. A Stored Communications Act order is sent to the service provider, who is directed to collect the documents in question and turn them over to the Government, unlike a traditional search warrant in which the Government itself identifies and seizes the documents or tangible property. *See* 18 U.S.C. § 2703(d). Because a Stored Communications Act warrant requires the provider to help execute the warrant by gathering the information, federal law expressly grants it the right to move to quash the warrant, *see id.*, just as the provider could move to quash a subpoena duces tecum. In sum, under “the mode of analysis which [the Court of Appeals] has consistently adhered to in deciding whether a proceeding is criminal or civil,” *Abrams*, 62 N.Y.2d at 193, the order under review is civil because it is akin to a motion to quash a subpoena.

2. The denial of the motion to quash is appealable for an additional reason: Facebook is not a potential defendant, and it is well settled New York law that a third party may appeal orders directing it to produce documents for use in a criminal proceeding. Because such an order is final as to that third party—and

because the third party would be unable to challenge the order by appealing the judgment in the criminal proceeding where it is not a defendant—New York courts have long treated such orders as exceptions to the general rule against interlocutory appeals during criminal proceedings.

In *People v. Marin*, for example, the court allowed a third-party law firm to take an immediate appeal from the denial of its motion to quash a subpoena duces tecum. *See* 86 A.D.2d 40 (2d Dep’t 1982). The court began by recognizing the general rule that “no appeal may be taken by either of the immediate parties to an underlying criminal action from a denial of an application to quash a trial subpoena duces tecum, since the propriety of such an order can be resolved on the direct appeal from any resulting judgment of conviction.” *Id.* at 42. However, the court explained, that “avenue of relief is totally unavailable to [the third party law firm], who is clearly aggrieved by the [trial court’s] order.” *Id.* Therefore, the court concluded, “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.*

This Court recognized the same principle in *People v. Bagley*, 720 N.Y.S.2d 454, 454 (1st Dep’t 2001), where it held that “[s]ince the Police Department was not a party to the underlying criminal action, it may properly appeal from the order denying the motion to quash the subpoena duces tecum.” And in *People v. Purley*,

this Court held that an order arising out of a criminal proceeding was “appealable because [the appellant], as a non-party, would otherwise be precluded from vindicating its position before an appellate body.” 297 A.D.2d at 501.

The same considerations apply to this case. Because Facebook cannot challenge the constitutionality of the warrants on appeal from any criminal trial that may ensue (as Facebook would not be a defendant), deeming the denial of Facebook’s motion to quash a non-appealable order would “preclude [Facebook] from any opportunity to vindicate its position before an appellate body.” *Marin*, 86 A.D.2d at 42. It cannot be the law that Facebook has no opportunity to appeal a court order commanding it to search for and collect peoples’ private information so that it can be turned over to the Government—and further commanding Facebook never to mention what the Government has forced it to do. Moreover, it is overwhelmingly likely that not all of the nearly 400 targeted individuals will ultimately end up charged with a crime—indeed, the indictments charge only 62 of the targeted individuals. It is a virtual certainty that at least *some* of the warrants would be forever insulated from appellate review if Facebook is not allowed an appeal. *See B. T. Prods., Inc. v. Barr*, 44 N.Y.2d 226, 232-34 (1978) (“To allow the failure to prosecute, a failure which may well be due to the absence of sufficient grounds to prosecute, to serve as a shield for the allegedly illegal seizure and retention of private property by government agents would be to make a

mockery of justice.”). The only possible consideration against allowing an appeal—that it would delay the Government’s investigation—is not applicable here, as Facebook has already complied with the warrants, and the Government’s recent indictment establishes that it has in no way been hindered by Facebook’s constitutional challenge.

Finally, this dispute remains live notwithstanding Facebook’s compliance or the recent indictment of 62 individuals.⁵ If Facebook prevails on the appeal, the Government will be required to return the seized information at issue and will not be able to use it during its investigation or any resulting prosecutions. *See Matter of Grand Jury Subpoenas*, 72 N.Y.2d 307, 311-12 (1988) (dispute is not moot where the seized materials “remain under the control of the Assistant District Attorney and continue to be used by him in the investigation”). Moreover, Facebook remains subject to the gag provisions, which violate Facebook’s First Amendment rights against content-based prior restraints on speech by indefinitely barring Facebook from disclosing any information about the search warrants to hundreds of its targeted users. And even if this Court were still inclined to question whether this remains a live dispute, it may exercise its discretionary

⁵ In moving for a stay pending appeal, Facebook argued that a stay was necessary because the production of user records would moot the appeal as to the Fourth Amendment issues. *See* 9/23/2013 Mot. to Stay at 6. This Court implicitly rejected the mootness argument in denying a stay.

authority “to review a case if the controversy or issue involved is likely to recur, typically evades review, and raises a substantial and novel question.” *Saratoga Cty. Chamber of Commerce v. Pataki*, 100 N.Y.2d 801, 811 (2003). All three factors are satisfied here, as this case presents important and recurring questions of constitutional law that often evade review because users are not even aware that the Government has swept up their private information.

B. Facebook Has Standing To Challenge The Warrants.

The trial court stated that Facebook lacked standing to challenge the warrants because “it is the Facebook subscribers who could assert an expectation of privacy in their postings,” not Facebook itself. A6 (Order at 3). That determination is erroneous, as Facebook has established standing in many ways.

First, “[t]he question of standing to challenge particular governmental action may, of course, be answered by the statute at issue, which may identify the class of persons entitled to seek review.” *Soc’y of Plastics Indus., Inc. v. Cnty. of Suffolk*, 77 N.Y.2d 761, 769 (1991). Here, the Stored Communications Act expressly grants Facebook standing to challenge the warrants.⁶ The Act provides:

⁶ The trial court repeatedly invoked and relied upon the Stored Communications Act as providing the necessary authority for the bulk warrants. *See* A5 (Order at 2) (“[u]nder Federal law, the court is authorized to issue search warrants targeting digital information pursuant to 18 U.S.C. § 2703”); A5 (emphasizing that the Government “has followed all the requisite procedures outlined in 18 U.S.C. § 2703(d) and N.Y. C.P.L. § 690.35 with regard to obtaining a court

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.

18 U.S.C. § 2703(d). The Senate Report accompanying this provision explained:

“This specific standing for the service provider to contest an overly broad order is intended to protect the service provider from unduly burdensome requirements and to permit an impartial judicial officer to evaluate the appropriateness of the government’s request.” S. Rep. No. 99-541, at 39 (1986). New York courts have recognized that this provision grants service providers like Facebook standing to move to quash orders issued under the Stored Communications Act. *See, e.g., People v. Harris*, 949 N.Y.S.2d 590, 593 (N.Y. Crim. Ct. 2012).

Second, Facebook has suffered an “injury in fact” from the bulk warrants and the Order. *See Soc’y of Plastics*, 77 N.Y.2d at 772 (describing an “injury in fact” as the “touchstone” for standing). Facebook was forced to conduct a burdensome search for the requested information and turn it over to the Government; if it did not, it faced civil and criminal contempt sanctions. That burden alone is sufficient to establish standing, just as a party forced to gather

order to search and seize digital information stored by Facebook”); A11-12 (Search Warrant at 3-4 (issuing gag order “pursuant to 18 U.S.C. § 2703(b)”).

documents in response to a subpoena has standing to challenge the subpoena. *See Marin*, 86 A.D. 2d at 42.

Facebook has suffered an additional injury in fact through the gag provisions that enjoin Facebook from speaking publicly about the warrants or even disclosing their existence to Facebook's users. *See* A11-12 (Search Warrant at 3-4) (“[T]his court orders Facebook not to notify or otherwise disclose the existence or execution of this warrant/order to any associated user/account holder”). It is beyond dispute that a party subject to a court-ordered restriction on speech has standing to challenge that order. *See, e.g., Nebraska Press Ass’n v. Stuart*, 427 U.S. 539, 546, 559 (1976).

Third, Facebook has standing to assert the rights of nearly 400 of its users targeted by the bulk warrants. The doctrine of third-party standing “allows a third party who has suffered an ‘injury in fact’ to assert the constitutional rights of others.” *New York Cnty. Lawyers’ Ass’n v. State of New York*, 294 A.D.2d 69, 74 (1st Dep’t 2002) (citations omitted). Courts consider three factors in determining whether a party may invoke third-party standing: “(1) the presence of some substantial relationship between the party asserting the claim and the rightholder, (2) the impossibility of the rightholder asserting his own rights, and (3) the need to avoid a dilution of the parties’ constitutional rights.” *Id.* at 75. Here, there plainly is a “substantial relationship” between Facebook and its users. Moreover, it is

impossible for the rightholders to assert their own rights because the majority of the nearly 400 individuals targeted have not been charged, and none of these individuals are aware of the bulk warrants' existence (and likely never will be, unless they are ultimately charged). Recognizing Facebook's third-party standing will avoid diluting the constitutional rights of hundreds of individuals whose personal information has now been seized by the Government without their knowledge. Because Facebook's interest in vindicating those rights is fully aligned with the interests of its users, Facebook is particularly well positioned to challenge the constitutionality of the bulk warrants.

The Government contended below that "any person aggrieved by any of these searches will have ample opportunity to litigate the issues raised by Facebook, and other relevant issues such as standing, during the subsequent criminal proceedings." A54 (9/22/2013 Eckenwiler Aff., Ex. 4 at 2); *see also* A57 (9/22/2013 Eckenwiler Aff., Ex. 4 at 5); A119 (10/2/2013 Eckenwiler Aff., Ex. 1 at 25). In response, Facebook explained that the Government's contention rested on the doubtful premise "that every one of the nearly 400 people who maintain these accounts will be criminally charged and have the opportunity to challenge these seizures" and that such a presumption was flawed because it was unlikely that the Government had already made charging decisions for each individual targeted. A60 (9/22/2013 Eckenwiler Aff., Ex. 5 at 2); *see also* A124 (10/2/2013 Eckenwiler

Aff., Ex. 1 at 30). Facebook argued that “[t]hose not ultimately charged will have no remedy for—or even knowledge of—the unlawful intrusions.” A60 (9/22/2013 Eckenwiler Aff., Ex. 5 at 2); *see also* A124 (10/2/2013 Eckenwiler Aff., Ex. 1 at 30). The Government declined to respond to this specific point below. *See* A129 (10/2/2013 Eckenwiler Aff., Ex. 1 at 35). Now, the indictments have been filed and the reality of the situation is clear: hundreds of people whose Facebook information was seized have not been charged with any crime. Under the Government’s approach, it could seize personal, private digital information of thousands of people—and only those individuals who are criminally charged would have an opportunity to contest the seizure, leaving no remedy for persons not ultimately charged or without knowledge of the Government’s unlawful intrusion.

II. THE BULK WARRANTS ARE UNCONSTITUTIONAL.

A. The Warrants Violate The Fourth Amendment.

The bulk warrants authorize the very sort of general search the Fourth Amendment forbids. The warrants require the seizure of personal information that has nothing to do with the crimes under investigation.

1. The Fourth Amendment’s Protections Apply With Particular Force In The Digital Age.

The Fourth Amendment provides:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be

violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV. The Fourth Amendment “safeguard[s] the privacy and security of individuals against arbitrary invasions by government officials.”

Camara v. Mun. Ct. of City & Cnty. of San Francisco, 387 U.S. 523, 528 (1967).⁷

“The chief evil that prompted the framing and adoption of the Fourth Amendment was the ‘indiscriminate searches and seizures’ conducted by the British ‘under the authority of general warrants.’” *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013) (quoting *Payton v. New York*, 445 U.S. 573, 583 (1980)). General warrants allowed “wide-ranging exploratory searches,” *Maryland v. Garrison*, 480 U.S. 79, 84 (1987), and gave the Government “unbridled discretion to rummage at will among a person’s private effects,” *Arizona v. Gant*, 556 U.S. 332, 345 (2009).

To achieve the Framers’ “manifest purpose” of “prevent[ing] general searches,” the Fourth Amendment “limit[s] the authorization to search to the specific areas and things for which there is probable cause to search.” *Garrison*,

⁷ The bulk warrants also violate Article I, Section 12, of the New York Constitution. Because the protections of Article I, Section 12, are identical to those afforded by the Fourth Amendment, *Harris*, 77 N.Y.2d at 437, all the arguments presented herein apply with regard to the New York Constitution as well.

480 U.S. at 84. This limitation is enshrined in the particularity requirement, which requires that the warrant “clearly state what is sought.” *United States v. Cioffi*, 668 F. Supp. 2d 385, 390 (E.D.N.Y. 2009). “[A] failure to describe the items to be seized with as much particularity as the circumstances reasonably allow offends the Fourth Amendment because there is no assurance that the permitted invasion of a suspect’s privacy and property are no more than absolutely necessary.” *Galpin*, 720 F.3d at 446 (quotation marks omitted). Moreover, the warrant “must specify the items to be seized by their relation to designated crimes.” *Id.* (quotation marks omitted). The description of the things to be seized must be “confined in scope to particularly described evidence relating to a specific crime for which there is demonstrable probable cause.” *In the Matter of Applications for Search Warrants for Information Associated with Target Email Accounts/Skype Accounts*, 2013 WL 4647554, at *5 (D. Kan. Aug. 27, 2013) (quotation marks omitted). Thus, “[a] warrant is overly broad if it does not contain sufficiently particularized language that creates a nexus between the suspected crime and the things to be seized.” *Id.*

These bedrock Fourth Amendment principles apply with particular force in the digital age, where massive amounts of private information can be captured in an instant. Computers “are postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more.” Orin S. Kerr, *Searches and Seizures in a Digital World*,

119 Harv. L. Rev. 531, 569 (2005). And because a computer can “store and intermingle a huge array of one’s personal papers in a single place,” *Otero*, 563 F.3d at 1132, the seizure of a computer, a hard drive, or the contents of a Facebook account can easily amount to a general search of one’s home and belongings. For this reason, courts have correctly warned that “[c]omputer search warrants are the closest things to general warrants we have confronted in this history of the Republic.” *In re Appeal of Application for Search Warrant*, 71 A.3d 1158, 1175 (Vt. 2012) (quoting P. Ohm, Response, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 Va. L. Rev. in Brief 1, 11 (2011)).

The Second Circuit has recognized the dangers of such warrants in the digital context. It has emphasized that, in light of the “serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant,” digital searches require a “heightened sensitivity” to constitutional concerns and limitations. *Galpin*, 720 F.3d at 447 (quotation marks omitted). Indeed, the court has specifically warned that “[t]he potential for privacy violations occasioned by an unbridled, exploratory search” is “compounded by the nature of digital storage.” *Id.* Other courts have reached the same conclusion. *See, e.g., Otero*, 563 F.3d at 1132 (“The modern development of the personal computer . . . increases law enforcement’s ability to conduct a wide-ranging search into a person’s private affairs, and accordingly

makes the particularity requirement that much more important.”). The Second Circuit recently concluded that a warrant authorizing the Government to retain all available data on an individual’s computer “on the off-chance the information would become relevant to a subsequent criminal investigation . . . would be the equivalent of a general warrant.” *United States v. Ganius*, 2014 WL 2722618, at *10 (2d Cir. June 17, 2014).

2. The Bulk Warrants Are Overbroad, Lack Particularity, And Authorize General Searches.

The trial court examined the warrants under Fourth Amendment standards, concluding that they “[i]mplicitly” passed constitutional muster. A7 (Order at 4). The trial court’s holding is erroneous. The bulk warrants are constitutionally defective in many respects.

The Bulk Warrants are overbroad and do not satisfy the particularity requirement. The bulk warrants require the search and seizure of virtually *all* records and information concerning 381 Facebook accounts, including “[a]ny and all subscriber and account information,” “all undeleted or saved photos,” “[a]ny and all associated ‘Groups,’” “[a]ny public or private messages,” “[a]ll notes,” and on and on. A9-10 (Search Warrant at 1-2). The warrants use precisely the sort of “broad catch-all phrase[s],” *United States v. George*, 975 F.2d 72, 75 (2d Cir. 1992), that signal overbreadth and a lack of particularity. A warrant that “allow[s] a search of all computer records without description or limitation . . . would not

meet the Fourth Amendment’s particularity requirement,” *United States v. Burgess*, 576 F.3d 1078, 1091 (10th Cir. 2009), and the warrants in this case do not.

Nor do the warrants contain a “temporal limitation on the items to be searched.” *United States v. Zemlyansky*, 945 F. Supp. 2d 438, 459 (S.D.N.Y. 2013). “[A] temporal limitation is an indicium of particularity,” and “a warrant’s failure to include a time limitation, where such limiting information is available and the warrant is otherwise wide-ranging, may render it insufficiently particular.” *Id.* (internal punctuation and citations omitted). Here, the Government essentially demanded the production of anything nearly 400 people have ever done on Facebook from the moment they created their accounts.⁸

The warrants demand private information that cannot possibly have any relevance to the Government’s investigation. Although the Government has not shown Facebook the 93-page affidavit submitted to establish probable cause for the warrants, that affidavit cannot possibly justify the seizure of *every* single message, photo, friend, “Like,” group membership, and communication by each of the 381 targeted accounts. A demand for essentially every action that nearly 400 users

⁸ The *one* date restriction—limiting the demand for IP logs to those created between January 1, 2010 and June 30, 2013—only highlights the problem, in that the Government provided *no* date restrictions as to the other 23 categories of information demanded. *See* A3-4 (Search Warrant at 1-2).

have taken since the moment they opened their Facebook accounts is “broader than can be justified by the probable cause upon which the warrant[s are] based.”

Galpin, 720 F.3d at 446. The fact that someone may “Like” the New York Giants or has professed their love for their children is extremely unlikely to have any bearing on the criminal investigation.

Indeed, the Government’s indictments confirm the unconstitutional breadth of the bulk warrants. It is clear that the Government, having focused on Facebook photographs of the targeted users acting in a manner allegedly inconsistent with their claimed disabilities, overreached in its unnecessary search and seizure of irrelevant and personal information. There was no need for the Government to search and seize content—such as private messages with friends or loved ones, or group memberships—that had no connection to the crimes alleged. It is inconceivable that *all* of the Facebook user information searched, seized, and held for nearly 400 Facebook users was and continues to be relevant or necessary to the Government’s case.

By their broad categories, sweeping language, and all-inclusive demands for the entirety of the targeted individuals’ activity on Facebook, these carbon copy bulk warrants authorize the very sort of general and indiscriminate search the Fourth Amendment forbids. Courts have rejected similar attempts by the Government to seize electronic information using overbroad search warrants. In

United States v. Barthelman, 2013 WL 3946084, at *11 (D. Kan. July 31, 2013), for example, the court held that search warrants directed at Yahoo! and Apple were overbroad and lacked particularity when they “allow[ed] the search of all emails, pictures, friends and groups.” Notably, the warrants in that case were narrower than the warrants at issue here, in that they were limited to a six-month time frame. *Id.*

Similarly, in *In re Search Warrants for Information Associated with Target Email Address*, 2012 WL 4383917, at *8 (D. Kan. Sept. 21, 2012), the court held that search warrants directed at Yahoo! under the Stored Communications Act lacked meaningful limitations and were overbroad. The court explained that the demand that Yahoo! produce “all email” associated with a particular account, along with “all records and other information regarding the account,” was “too broad and too general.” *Id.* The warrants in this case are even more troubling: they seek all communications and account information involving the targeted users.

Most recently, in *In the Matter of the Search of Information Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.*, 2014 WL 1377793, at **1, 3 (D.D.C. Apr. 7, 2014), the court denied the Government’s effort to search and seize a single email account. The court explained that the request amounted to an impermissible general warrant because the Government

made no effort to limit its search to information relevant to the crimes under investigation. “[I]f this were the physical world,” the court explained, the warrant “would be akin to a warrant asking the post office to provide copies of all mail ever sent by or delivered to a certain address so that the government can open and read all the mail to find out whether it constitutes fruits, evidence or instrumentality of a crime. The Fourth Amendment would not allow such a warrant.” *Id.* at *5 (quotation marks omitted); *see also* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 *Stan. L. Rev.* 1005, 1014 (2010) (“Unlike physical evidence, electronic data has no inherent limitations on how much can exist, where it can be located, and where it can be stored.”).

The same is true here. The bulk warrants do not “link the items to be searched and seized to the suspected criminal activity,” thus failing to provide “meaningful parameters on an otherwise limitless search.” *United States v. Rosa*, 626 F.3d 56, 62 (2d Cir. 2010). Instead, after reciting 24 broad categories of data from the 381 individual accounts, the warrants assert in conclusory fashion: “[T]here is reasonable cause to believe that the above-described property constitutes evidence and tends to demonstrate that an offense was committed, including but not limited to” grand larceny, offering a false instrument for filing, and conspiracy to commit these crimes. *See* A11 (Search Warrant at 3). Missing from the warrant is any *link* between the items to be seized and the alleged crimes;

the purpose of the nexus requirement is to narrow the search by excluding items that are plainly irrelevant. By stating that *all* of the information in 24 broad categories is “evidence” of “larceny” (or related crimes)—a statement that cannot possibly be true—the warrants are “not narrowed by any references to the crimes committed.” *Zemlyansky*, 945 F. Supp. 2d at 455. As the Second Circuit has stated, “[m]ere reference to ‘evidence’ of a violation of a broad criminal statute or general criminal activity provides no readily ascertainable guidelines for the executing officers as to what items to seize.” *George*, 975 F.2d at 76. Including an “unadorned reference” to broad statutes that can encompass a variety of offenses, as the Government has done here, “does not sufficiently limit the scope of a search warrant.” *United States v. Leary*, 846 F.2d 592, 602 (10th Cir. 1988).⁹

The court in the recent *Skype* case confronted a similar problem: sweeping requests for electronic information that were not specifically linked to the crimes under investigation. *See Skype*, 2013 WL 4647554, at **7-8. The court explained that “[t]he warrants fail to set any limits on the email communications and

⁹ Any details contained in the investigator’s affidavit cannot salvage the defective warrant because the affidavit is neither attached to the warrant nor incorporated by reference. *See Groh v. Ramirez*, 540 U.S. 551, 557 (2004) (“The fact that the *application* adequately described ‘the things to be seized’ does not save the *warrant* from its facial invalidity. The Fourth Amendment by its terms requires particularity in the warrant, not in the supporting documents.”) (emphases in original).

information that the electronic communications service provider is to disclose to the government, but instead require each Provider to disclose all email communications in their entirety and all information about the account without restriction.” *Id.* at *8. “Most troubling,” the court continued, is that “the warrants fail to limit the universe of electronic communications and information to be turned over to the government to the specific crimes being investigated.” *Id.* The same is true in this case. The warrants’ failure to identify any specific wrongful transaction to which the documents are related violates the Fourth Amendment.

There are no procedures to require the return of the seized information. The bulk warrants are constitutionally defective for an additional reason: they do not contain any provisions requiring the Government to return the vast amounts of seized information that have nothing to do with the crimes being investigated. The omission of these provisions makes the Government’s seizure unlawfully co-extensive with its search.

The Second Circuit recently held that the Fourth Amendment does not permit officials executing a warrant for the seizure of electronic data to indefinitely retain such data. *Ganias*, 2014 WL 2722618, at *10. The court explained that “[i]f the Government could seize and retain non-responsive electronic records indefinitely, . . . every warrant to search for particular electronic data would become, in essence, a general warrant.” *Id.* at *11.

Similarly, in *In the Matter of the Search of Information Associated with the Account Identified by the Username Aaron.Alexis*, 2013 WL 7856600, at *7 (D.D.C. Nov. 26, 2013), the court held that the warrants at issue were defective because they failed to include provisions for the return of the information seized by the Government. The court emphasized that a warrant (or a court order approving the warrant) *must* include provisions prohibiting the Government from “collecting and keeping indefinitely information to which it has no right.” *See also id.* (citing *In the Matter of the Search of Information Associated with [Redacted] That Is Stored at Premises Controlled by Yahoo! Inc.*, No. 13-MJ-728 (D.D.C. Sept. 25, 2013) (issuing order requiring Government to return or destroy seized electronic records not relevant to investigation)); *see also In re: [REDACTED]@gmail.com*, No. 5:14-mj-70655-PSG, at 6 (N.D. Cal. May 9, 2014) (denying warrant application and emphasizing that the “the government [has not] made any kind of commitment to return or destroy evidence that is not relevant to its investigation”); *Apple*, 2014 WL 1377793, at *8 (“[I]f the government seizes data it knows is outside the scope of the warrant, it must either destroy the data or return it. It cannot simply keep it.”). As the Ninth Circuit’s Judge Kozinski has explained, “the warrant application should normally include, or the issuing judicial officer should insert, a protocol for preventing agents involved in the investigation from examining or retaining any data other than that for which probable cause is

shown.” *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1179 (9th Cir. 2010) (Kozinski, *J.*, concurring).

Here, even though the bulk warrants were issued pursuant to the Stored Communications Act, the trial court refused to apply the two-step process required under Federal Rule of Criminal Procedure 41(e)(2)(B) and commonly employed in electronic searches. Under that approach, the Government is required to first “search” the information collected under the warrant, and then “seize” the subset of information it deemed relevant. *See Aaron Alexis*, 2013 WL 7856600, at *6 (following two-step approach). That procedure was not followed here. Instead, the court allowed the Government to seize and permanently retain *all* of the information falling within the 24 broad categories in the bulk warrants, even though only a small sliver of that information could possibly constitute evidence of the crimes for which probable cause was found. The Facebook user information searched, seized, and copied by the Government should not be held indefinitely by the District Attorney’s Office. It must be returned to Facebook or destroyed. Because the court failed to include any provisions requiring the Government to return or destroy irrelevant information, the bulk warrants are constitutionally invalid for that reason as well.

B. The Bulk Warrants’ Indefinite Gag Provisions Violate The Stored Communications Act And The First Amendment.

The bulk warrants contain gag provisions barring Facebook from disclosing their existence or publicly speaking about them. The gag provisions currently apply to 302 of the targeted Facebook users and have an indefinite duration—they will continue forever unless the court or the Government says otherwise. *See* A11-12 (Search Warrant at 3-4) (“[T]his court orders Facebook not to notify or otherwise disclose the existence or execution of this warrant/order to any associated user/account holder”); A8 (Order at 5) (“The Nondisclosure Order remains in effect until the court orders otherwise.”). The gag provisions are not authorized by the Stored Communications Act and are unconstitutional.¹⁰

1. The Gag Provisions Violate The Stored Communications Act.

The trial court issued the gag orders under the Stored Communications Act, 18 U.S.C. § 2705(b). *See* A11 (Search Warrant at 3).¹¹ But while Section 2705(b)

¹⁰ Although the trial court asserted that New York law also granted it the power to order nondisclosure, A10 (Order at 4), the gag provisions were imposed “pursuant to” the Stored Communications Act, not any provision of state law, *see* A5 (Search Warrant at 3). New York law does not authorize indefinite gag orders in any event. Indeed, the court did not view its state-law authority as permitting a gag order that extended beyond the conclusion of the grand jury investigation. *See* A10 (Order at 4) (under state law, court may impose gag order “to protect the existence of evidence subject to an ongoing Grand Jury investigation”).

¹¹ The trial court erroneously cited Section 2703(b) as the source of its authority.

permits courts to require nondisclosure for limited periods, it does *not* authorize indefinite gag orders. The plain language of the statute makes this clear: it provides that a nondisclosure order may not be permanent, but may extend only “for such period as the court deems appropriate.” 18 U.S.C. § 2705(b) (emphasis added). In this context, a “period” is a unit of time with a beginning and an end; it does not refer to an open-ended, limitless mandate.

The five factors that a court must consider before issuing a nondisclosure order reinforce this point. Those factors—which include potential destruction of evidence, jeopardizing an ongoing investigation, and so forth, *see* 18 U.S.C. § 2705(b)(1)-(5)—carry no weight once the investigation has concluded or once a prosecution has begun. Indeed, once an indictment has been announced, there can be no possible justification for maintaining the gag order, as the existence of the investigation will already have been made public.

The Government made no effort to establish that these factors supported entering a gag order of indefinite, and potentially permanent, duration. The warrants themselves assert only that disclosure “could cause individuals to flee, destroy evidence, or otherwise interfere with an ongoing criminal investigation.” A12 (Search Warrant at 4). In fact, the Government acknowledged in the trial court that once the “ongoing investigation” has run its course, “the need for secrecy [will have] passed.” A57 (Gov’t Opp. to Mot. to Quash at 5).

Even if the Government could show that absent a gag order the potential harms would ensue during the pendency of its investigation, it could not show—and did not show—that these harms would ensue five years in the future. The trial court thus erred, and exceeded its authority under the Stored Communications Act, by approving indefinite nondisclosure provisions rather than limiting their duration to an appropriate “period,” as the statute requires. *See* 18 U.S.C. § 2705(b).¹²

2. The Gag Provisions Violate The First Amendment.

The gag provisions also violate the First Amendment because they are an indefinite, content-based restriction on Facebook’s speech concerning a matter of public interest and importance.

The court in *In re Sealing*, 562 F. Supp. 2d 876, 878 (S.D. Tex. 2008), held that “setting a fixed expiration date on sealing and non-disclosure of electronic surveillance orders is not merely better practice, but required by law: in particular, the First Amendment prohibition against prior restraint of speech and the common law right of public access to judicial records.” There, just as in this case, the Government demanded information under the Stored Communications Act, and

¹² Even if the statute could plausibly be read to allow gag orders of indefinite duration, this Court should not adopt an interpretation that raises serious constitutional questions, as shown below. *See Clark v. Martinez*, 543 U.S. 371, 381 (2005) (when there are “competing plausible interpretations of a statutory text,” Congress most likely “did not intend the alternative which raises serious constitutional doubts”).

sought an order indefinitely prohibiting the service provider from disclosing the Government’s request. The court observed that “[t]he practice of issuing secret electronic surveillance orders without an expiration date raises troubling legal questions,” noting that “[i]f the recipients of [such] orders are forever enjoined from discussing them, the individual targets may never learn that they had been subjected to such surveillance, and this lack of information will inevitably stifle public debate about the proper scope and extent of this important law enforcement tool.” *Id.* at 880, 882. Holding that a content-based restriction like the gag order must be subjected to “rigorous scrutiny” under the First Amendment, the court concluded that:

An indefinite non-disclosure order is tantamount to a permanent injunction of prior restraint. To the extent such an order enjoins speech beyond the life of the underlying investigation, it must be narrowly tailored to serve a compelling governmental interest in order to pass muster under the First Amendment. The governmental interests considered here—the integrity of an ongoing criminal investigation, the reputational interests of targets, and the sensitivity of investigative techniques—are not sufficiently compelling to justify a permanent gag order.

Id. at 882, 886. The court’s conclusion tracked the Supreme Court’s decision in *Butterworth v. Smith*, 494 U.S. 624 (1990), which held that “a Florida grand jury statute violated the First Amendment insofar as it prohibited a grand jury witness from disclosing his own testimony after the grand jury investigation ended.” *In re Sealing*, 562 F. Supp. 2d at 883; *see Butterworth*, 494 U.S. at 632-33 (“When an

investigation ends, there is no longer a need to keep information from the targeted individual in order to prevent his escape—th[e] individual will presumably have been exonerated, on the one hand, or arrested or otherwise informed of the charges against him, on the other.”).

The same reasoning applies here. Once the Government’s investigation has ended, there is no need to keep the existence of the bulk warrants secret. The targets of the investigation will either have been charged or exonerated. There is no danger of a classified evidence-gathering method being revealed. On the other hand, maintaining an indefinite ban on disclosure will stifle public debate over this important issue. The question whether the Government’s electronic surveillance and evidence-gathering tactics have gone too far is the subject of a vigorous and robust national debate, particularly in the wake of the recent orders in the NSA surveillance cases. *See ACLU v. Clapper*, 959 F. Supp. 2d 724, 730 (S.D.N.Y. 2013).

For all these reasons, this Court should conclude that the gag provisions violate the First Amendment.

CONCLUSION

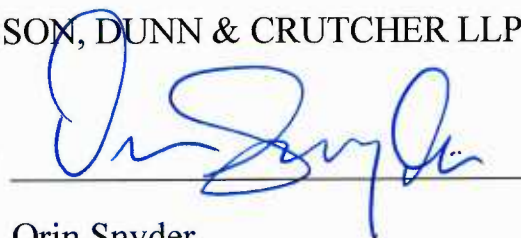
This Court should reverse the Order and quash the bulk warrants.

Dated: New York, New York
June 20, 2014

Respectfully submitted,

GIBSON, DUNN & CRUTCHER LLP

By: _____



Orin Snyder
osnyder@gibsondunn.com
Alexander H. Southwell
asouthwell@gibsondunn.com
Jane Kim
jkim@gibsondunn.com
200 Park Avenue
New York, New York 10166
Telephone: (212) 351-4000

Thomas H. Dupree, Jr.
(*pro hac vice* pending)
tdupree@gibsondunn.com
1050 Connecticut Avenue, NW
Washington, DC 20036
Telephone: (202) 955-8500

Attorneys for Facebook, Inc.

PRINTING SPECIFICATIONS 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(I)
- 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 9,786 words.

Dated: New York, New York
June 20, 2014

Respectfully submitted,
GIBSON, DUNN & CRUTCHER LLP

By: 

Jane Kim
jkim@gibsondunn.com
200 Park Avenue
New York, New York 10166
Telephone: (212) 351-4000

Attorney for Facebook, Inc.

AFFIRMATION OF SERVICE

JANE KIM, an attorney duly admitted to practice law in the Courts of this State, hereby subscribes and affirms as true, under penalty of perjury pursuant to N.Y. C.P.L.R. § 2106, as follows:

1. I am an attorney associated with the law firm of Gibson, Dunn & Crutcher LLP, 200 Park Avenue, New York, New York, (212) 351-4000. I am an Attorney for Facebook, Inc. I am not a party to this proceeding and I am over 18 years of age.

2. On the 20th day of June, 2014, I caused two (2) true and correct copies of the Brief of Appellant Facebook, Inc., with Printing Specifications Statement, as well as two (2) true and correct copies of the Appendix and the Compendium of Authorities accompanying the Brief, to be served by hand delivery upon the following counsel of record:

Bryan Serino, Assistant District Attorney
NEW YORK COUNTY DISTRICT ATTORNEY'S OFFICE
One Hogan Place
New York, New York 10013

Dated: New York, New York
June 20, 2014



Jane Kim