ATTACHMENT A

IN THE UNITED STATES DISTRICT COURT FILED
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

2011 JAN 18 P 12:58

IN RE 2703(d) ORDER AND 2703(f) PRESERVATION REQUEST RELATING TO GMAIL ACCOUNT [redacted]	)	Misc. No. 10GJ3793 CLERK US DISTRICT COURT ALEXANDRIA, VIRGINIA
	)	FILED UNDER SEAL

GOOGLE INC.'S MOTION TO MODIFY 2703(d) ORDER FOR PURPOSE OF PROVIDING NOTICE TO USER AND MEMORANDUM IN SUPPORT

I. INTRODUCTION

This matter involves a grand jury investigation of the Wikileaks publication of State Department cables and related matters. The fact of the investigation has been widely reported in the *New York Times* and other news publications, across the Internet and around the globe.[1] Demands have been made to third party service providers, including Google Inc. ("Google"), seeking compelled disclosure of information such as with whom the subject users of those services communicated and which computers they used to do so. The Google Gmail user [redacted] is the subject of the demand at issue here (the "Order").[2] Because of the already public nature of the Wikileaks investigation, the fact that a nearly identical order to another provider involving the same account identifier has been unsealed by this Court in the same Grand Jury proceeding, and for other reasons set forth herein, Google requests permission to provide notice

[1] *See, e.g.*, Scott Shane and John F. Burns, *U.S. Subpoenas Twitter Over WikiLeaks Supporters*, N.Y. Times, Jan. 8, 2011, http://www.nytimes.com/2011/01/09/world/09wiki.html (last visited Jan. 13, 2011); Anthony Boadle, *U.S. orders Twitter to hand over Wikileaks records*, Reuters, Jan. 8, 2011, http://www.reuters.com/article/idUSTRE7071642011010 8 (last visited Jan. 14, 2011); Ravi Somaiya, *Release on Bail of WikiLeaks Founder Is Delayed by Appeal*, N.Y. Times, Dec. 14, 2010, *available at* http://www.nytimes.com/2010/12/15/world/europe/15assange.html?src=twrhp (last visited Jan. 3, 2011); *Assange attorney: Secret grand jury meeting in Virginia on WikiLeaks*, CNN Justice, Dec. 13, 2010, http://articles.cnn.com/2010-12-13/justice/wikileaks.investigation_1_julian-assange-wikileaks-case-grand-jury?_s=PM:CRIME (last visited Jan. 3, 2011); Dan Goodin, *Grand jury meets to decide fate of WikiLeaks founder*, The Register, Dec. 13, 2010, *available at* http://www.theregister.co.uk/2010/12/13/assange_grand_jury/ (last visited Jan. 3, 2011).

[2] *See* Declaration of John K. Roche, Ex. 1 ("Roche Decl.").

of the Order to that Gmail user and the user's attorney far enough in advance to give them a meaningful opportunity to contest the request.

II. FACTUAL BACKGROUND

A. Summary

The Order in this matter was issued on January 4, 2011, and seeks information about the Gmail user [redacted] A user with the account identifier [redacted] was also one of the targets of such an order issued on December 14, 2010 by this Court at the request of the government to Twitter pursuant to 18 U.S.C. § 2703(d) (the "Twitter Order").[3] Twitter asked the government to unseal that order so that it might give its users notice and an opportunity to assert any privileges or rights to prevent such disclosures. The government agreed to do so on January 3, 2010, and Magistrate Judge Buchanan entered an order to unseal on January 5th.[4]

Having agreed on January 3 to unseal one order to Twitter involving account information for the Twitter user [redacted] the next day the government procured this Order under seal from this Court to compel Google to produce the identical type of user information and records previously sought from Twitter for the Google Gmail account [redacted] for the same period of November 1, 2009 to the present. This Order contains the identical perpetual nondisclosure provision that was present in the Twitter Order, prohibiting Google from "disclos[ing] the existence of the application or this Order of the Court, or the existence of the investigation, to the listed subscriber or to any other person, unless and until authorized to do so by the Court."

[3] Roche Decl., Ex. 2.

[4] *Id.* Ex. 3.

Pursuant to Google's policy and having learned through the extensive coverage of the unsealed Twitter Order that [redacted] account records had been sought and that motions to object are imminently due from the Twitter users whose data has been requested, Google promptly notified the government that it too sought to notify its user of the Order.[5] The government declined to agree to a modification to allow this, purportedly because the Order involves a different investigation.[6] The government also served a preservation demand on Google, and likewise, the government has declined to permit Google to notify the user of the demand.[7]

Google respectfully submits that this Order, like the Twitter Order, may present substantial free speech concerns and may implicate journalistic and academic freedom. Furthermore, the government's investigation of Wikileaks generally, and its interest in the [redacted] user name specifically, is a matter of public record, thus obviating the need for this Order's nondisclosure provision. In addition, Google has preserved the requested records, thus there is no danger of loss or destruction of the information sought. Accordingly, Google requests that the Court modify this Order to permit notice of the Order and preservation request to be given to Google's user and attorney and that the user be given 20 days from the date of the Court's order to seek any relief.

Google takes no position regarding the propriety of Wikileaks' actions or the government's investigation. It seeks to provide notice to the user and his legal representative so that the user has an opportunity to be heard. Google has preserved responsive information to the extent it exists pending the Court's ruling on this motion.

---

[5] Roche Decl., ¶ 6.

[6] *Id.*

[7] *Id.*, Ex. 4.

B. Relevant Actors

Google provides electronic mail services to the public through its Gmail service. Google assiduously protects the privacy and free speech rights of its Gmail users, as evidenced by its opposition, with the support of the U.S. State Department, to the Chinese government's attack on the Gmail accounts of Chinese human rights activists.[8]

Google's general practice and preference, when addressing legal demands such as court orders, is to give notice to the account holders, whenever it is permissible and practical to do so. Even where the government asserts that disclosure to the user may have an adverse impact on an investigation, or where an order is sealed but nonetheless raises serious First Amendment concerns, Google may move to unseal the order or seek permission to notify its users.

Google recognizes that such notice is important because its users are better situated to assert their rights under the First Amendment or other applicable privileges and articulate their concerns to the Court. It is for those reasons that Google asks the Court to unseal the Order as the Court did for another provider in the same Grand Jury proceeding.

Wikileaks describes itself as a journalistic enterprise.[9] Whether Wikileaks does in fact consist of journalists or engage in journalism is a matter of public debate, and an issue upon which Google does not comment.

---

[8] Andrew Jacobs and Miguel Helft, *Google, Citing Attack, Threatens to Exit China*, N.Y. Times, Jan. 13, 2011, http://www.nytimes.com/2010/01/13/world/asia/13beijing.html?_r=1&pagewanted=print (last visited Jan. 13, 2011).

[9] *Salmeron v. Enterprise Recovery Systems, Inc.*, 579 F.3d 787, 791 n.1 (7th Cir. 2009) ("'[F]ounded by Chinese dissidents, journalists, mathematicians and startup company technologists, from the US, Taiwan, Europe, Australia and South Africa,' Wikileaks styles itself as 'an uncensorable version of Wikipedia for untraceable mass document leaking and analysis.' http:// wikileaks. org/ wiki/ Wikileaks: About (last visited July 16, 2009).").

Twitter is a real-time information network that has been described by one federal district court as "a social networking and micro-blogging service that invites its users to answer the question: 'What are you doing?'" *U.S. v. Shelnutt*, No. 4:09-CR-14 (CDL), 2009 WL 3681827, at *1 n.1 (M.D. Ga. Nov. 2, 2009) ("Twitter's users can send and read electronic messages known as 'tweets.' A tweet is a short text post (up to 140 characters) delivered through Internet or phone-based text systems to the author's subscribers. Users can send and receive tweets in several ways, including via the Twitter website.").

Although Google does not comment on and could not confirm whether the Twitter accoun[redacted]s controlled by the same user as the Gmail [redacted]account, it is instructive to note that in a "tweet," the Twitter user[redacted]ndicates that since at least mid-December 2010 [redacted]has been well aware that a government investigation is underway.[10]

C. Procedural Posture

The Twitter Order was issued on December 14, 2010 and relates to the ongoing Wikileaks investigation, which is obviously an issue of great public interest.[11] The Twitter Order demanded the production of subscriber information and certain records and other non-content information for a number of Twitter account holders from November 1, 2009 to the present, including an account with the user nam[redacted] It also contained a non-disclosure provision. The grand jury investigation underlying the Twitter Order was widely reported in the *New York*

[10] *See* [redacted] tweet of Dec. 17, 2010 @ 4:22 p.m. ("Unrelated to any travel issues - the FBI is now actively bothering my friends and questioning them inside the United States."), http://twitter.com[redacted]/status/15879462465835008 (last visited on Dec. 21, 2010); *see also* [redacted]' tweet of Jan. 7, 2011 @ 9:26 p.m. ("Note that we can assume Google & Facebook also have secret US government subpoenas. They make no comment. Did they fold?"), http://twitter.com[redacted]/ (last visited Jan. 18, 2011).

[11] Roche Decl., Ex. 2.

Times and other media outlets around the time the Twitter Order was issued.[12] Indeed, prior to issuance of the order, the Attorney General had acknowledged that the government was actively investigating Wikileaks.[13]

On January 5, 2011, upon motion by the government made at the behest of Twitter,[14] Magistrate Judge Buchanan unsealed the Twitter Order and authorized Twitter to disclose it to its users, including Twitter user [redacted]

In the days following January 5, 2011, the unsealed Twitter Order was posted on the Internet and widely discussed in the media.[16] On January 7, 2011, a "tweet" from Twitter user [redacted] stated that "we can assume Google & Facebook also have secret US government subpoenas."[17]

On January 4, 2011, the day after the government agreed to unseal the Twitter Order, it procured from this Court the Order in this matter, which is substantially identical to the Twitter

---

[12] Ravi Somaiya, *Release on Bail of WikiLeaks Founder Is Delayed by Appeal*, N.Y. Times, Dec. 14, 2010, http://www.nytimes.com/2010/12/15/world/europe/15assange.html?src=twrhp (last visited Jan. 3, 2011); *see also Assange attorney: Secret grand jury meeting in Virginia on WikiLeaks*, CNN Justice, Dec. 13, 2010, http://articles.cnn.com/2010-12-13/justice/wikileaks.investigation_1_julian-assange-wikileaks-case-grand-jury?_s=PM:CRIME (last visited Jan. 3, 2011); Dan Goodin, *Grand jury meets to decide fate of WikiLeaks founder*, The Register, Dec. 13, 2010, http://www.theregister.co.uk/2010/12/13/assange_grand_jury/ (last visited Jan. 3, 2011).

[13] Ellen Nakashima & Jerry Markon, *WikiLeaks founder could be charged under Espionage Act*, Wash. Post, Nov. 30, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/11/29/AR2010112905973.html (last visited Jan. 3, 2011).

[14] Perkins Coie LLP represents both Twitter and Google.

[15] Roche Decl., Ex. 3.

[16] *See, e.g.*, Scott Shane and John F. Burns, *U.S. Subpoenas Twitter Over WikiLeaks Supporters*, N.Y. Times, Jan. 8, 2011, http://www.nytimes.com/2011/01/09/world/09wiki.html (last visited Jan. 13, 2011); Anthony Boadle, *U.S. orders Twitter to hand over Wikileaks records*, Reuters, Jan. 8, 2011, http://www.reuters.com/article/idUSTRE70716420110108 (last visited Jan. 14, 2011).

[17] *See* [redacted] tweet of Jan. 7, 2011 @ 9:26 p.m. ("Note that we can assume Google & Facebook also have secret US government subpoenas. They make no comment. Did they fold?"), http://twitter.com[redacted] (last visited Jan. 18, 2011).

Order and compels Google to produce the identical information as the Twitter Order for the Google Gmail account [redacted].[18] The perpetual nondisclosure provision in the Order is identical to the Twitter Order nondisclosure provision.

On January 12, 2011, the government issued a preservation request pursuant to 18 U.S.C. § 2703(f) "for the preservation of all stored communications, records, and other evidence" in Google's possession regarding Gmail user [redacted] for November 2009 to the present.[19]

That same day, Google's outside counsel spoke with several government attorneys regarding the nondisclosure provisions in this Order.[20] Google's attorney notified the government that Google wished to immediately give notice of the Order to its user and requested that the government agree to so modify the Order.[21] The government declined Google's request saying only that the Order involves a different investigation than the one underlying the Twitter Order.[22] No further explanation was provided.[23] The government offered to release Google from the notice constraint 90 days after it produced, with a provision allowing the government to petition for a further extension.[24] Google consequently notified the government that it intended to file this motion to unseal the order and to modify its nondisclosure provisions so that Google

---

[18] *See* Roche Decl., Ex. 1.

[19] *Id.*, Ex. 4.

[20] *Id.*, ¶ 6.

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] *Id.*

could give immediate notice to its user.[25] Google's attorney and the government subsequently agreed on a schedule for filing and argument of this motion.

III. ARGUMENT

A. There is No Need for Secrecy of the Order or the Preservation Request

Nondisclosure orders are permitted in extraordinary circumstances under 18 U.S.C. § 2705. The Order in this matter relies upon the standard set forth in § 2705(b)(5), which provides for nondisclosure when notification will result in "seriously jeopardizing an investigation." Nondisclosure requests such as this are subject to the most demanding scrutiny, particularly when they are indefinite in scope:

> If the recipients of [surveillance] 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. By constricting the flow of information at its source, the government dries up the marketplace of ideas just as effectively as a customer-targeted injunction would do. Given the public's intense interest in this area of law, such content-based restrictions are subject to rigorous scrutiny.

In re Sealing and Non-Disclosure of Pen/Trap/2703(d) Orders, 562 F. Supp. 2d 876, 882 (S.D. Tex. 2008) (setting a default 180 day period for sealing and non-disclosure of electronic surveillance orders) (internal citations omitted).

Google is not privy to what showing the government made in the affidavit in support of the application for the Order. Given that the government moved to unseal an order to another provider requesting the identical type of information on an account with an identical identifier, it

[25] *See* Roche Decl., ¶ 6.

is difficult to understand how the government could meet the "seriously jeopardizing" standard in this case. The government's offer to release Google from the notice constraint after 90 days demonstrates that a limited nondisclosure provision could have been requested in the first place, and that this very public investigation is at or near an end, which further obviates the need for confidentiality.

Nor does the Order meet the traditional standard for grand jury confidentiality. Grand jury proceedings are traditionally confidential because

> if preindictment proceedings were made public, many prospective witnesses would be hesitant to come forward voluntarily, knowing that those against whom they testify would be aware of that testimony. Moreover, witnesses who appeared before the grand jury would be less likely to testify fully and frankly, as they would be open to retribution as well as to inducements. There also would be the risk that those about to be indicted would flee, or would try to influence individual grand jurors to vote against indictment. Finally, by preserving the secrecy of the proceedings, we assure that persons who are accused but exonerated by the grand jury will not be held up to public ridicule.

Finn v. Schiller, 72 F.3d 1182, 1187 n.6 (4th Cir. 1996) (quoting *Douglas Oil Co. v. Petrol Stops N.W.*, 441 U.S. 211, 219 (1979)). Of course, "it is a 'common-sense proposition that secrecy is no longer "necessary" when the contents of grand jury matters have become public.'" *McHan v. C.I.R.*, 558 F.3d 326, 334 (4th Cir. 2009) (quoting *In re Grand Jury Subpoena*, 438 F.3d 1138, 1140 (D.C. Cir. 2006)).

In this case, the grand jury's investigation of the Twitter user [redacted] is public record. Moreover, Google has preserved all records and content related to the Gmail user [redacted] account. Accordingly, there is no risk of destruction evidence, and none of the other interests served by the traditional secrecy of grand jury proceedings would be undermined in any way by disclosure of this Order or the preservation request.

B. The Order May Raise Significant Free Speech and Other Privilege Issues

Grand jury proceedings are not exempt from the limits of the First Amendment. *Branzburg v. Hayes*, 408 U.S. 665, 707-08 (1972). Accordingly, courts must "strike[] the essential balance between the purposes of the grand jury and the protections of the First Amendment" by requiring the grand jury to "show a strong possibility that the requested [information] will expose criminal activity." *In re Grand Jury Subpoena: Subpoena Duces Tecum*, 829 F.2d 1291, 1305 (4th Cir. 1987) (Wilkinson, J., concurring).

Shielded by the First Amendment, the press "has been a mighty catalyst in awakening public interest in governmental affairs, exposing corruption among public officers and employees and generally informing the citizenry of public events and occurrences." *Estes v. Texas*, 381 U.S. 532, 539 (1965). Hence, journalists are entitled to certain free speech protections in order "to ensure a free and vital press, without which an open and democratic society would be impossible to maintain." *Ashcraft v. Conoco, Inc.*, 218 F.3d 282, 287 (4th Cir. 2000). Likewise, "[o]ur Nation is deeply committed to safeguarding academic freedom, which is of transcendent value to all of us and not merely to the teachers concerned. That freedom is therefore a special concern of the First Amendment . . . ." *Keyishian v. Board of Regents of University of State of N. Y.*, 385 U.S. 589, 603 (1967).

To the extent that the Gmail user [redacted] is a journalist or enaged in other constitutionally protected activities, the user may wish to assert First Amendment rights or any applicable journalistic, academic or other privileges or defenses to which the user is entitled. Google is not properly positioned to do so on behalf of users.

The Department of Justice itself recognizes that "the prosecutorial power of the government should not be used in such a way that it impairs a reporter's responsibility to cover as broadly as possible controversial public issues," and has thus enacted special procedures for obtaining information from or about members of the news media. *See* 28 C.F.R. § 50.10; *see also* U.S. Attorney's Manual, § 9-13.400. Therefore, given the extraordinary controversy and newsworthiness surrounding Wikileaks' alleged actions, the applicability of any privilege may be heightened. *In re Grand Jury Subpoena, Judith Miller*, 438 F.3d 1141, 1164 (D.C. Cir. 2006 ("I believe that the consensus of forty-nine states plus the District of Columbia – and even the Department of Justice – would require us to protect reporters' sources as a matter of federal common law were the leak at issue either less harmful or more newsworthy.") (Tatel, J., concurring).

Had Gmail user [redacted] rather than Google, been the recipient of the Order or similar legal process, there is no doubt that the user would have the right to assert any objections directly. *Id.* at 1164 ("given that any witness – journalist or otherwise – may challenge [an unreasonable or oppressive] subpoena, the majority [in *Branzburg*] must have meant, at the very least, that the First Amendment demands a broader notion of 'harassment' for journalists than for other witnesses.") (Tatel, J., concurring). It is therefore within the sound discretion of the Court to modify the Order for the purpose of allowing Google to give notice to its affected user so that the user may decide whether to object to Google's production of the documents and information demanded therein.

IV. CONCLUSION

Google takes no position regarding the propriety of Wikileaks' alleged actions or the government's investigation, but given the extraordinary nature of the issues surrounding the

Wikileaks matter, Google requests only that the Court modify the Order to permit notice of the Order and preservation request to be given to Google's user and the user's attorneys. Google further requests that it be permitted to discuss the Order with its user and the user's attorneys and that the user be given 20 days from the date of the Court's order to file an appropriate response. In the meantime, Google has preserved responsive information, and will produce that information if its user does not file a motion or other pleading in opposition within 20 days of the Court's order.

DATED this 18th day of January, 2011.

Respectfully submitted,

By _____

John K. Roche (VSB# 68594)
Perkins Coie LLP
700 13th St., N.W., Suite 600
Washington, D.C. 20005-3960
Phone: 202-434-1627
Fax: 202-654-9106
JRoche@perkinscoie.com

Albert Gidari (*pro hac vice pending*)
Perkins Coie LLP
1201 Third Avenue, Suite 4800
Seattle, Washington 98101
Phone: 206-359-8000
Fax: 206-359-9000
AGidari@perkinscoie.com

Attorneys for Google Inc.

CERTIFICATE OF SERVICE

I hereby certify that on this 18th day of January, 2011, the foregoing document was sent via hand delivery and email to the following persons:

[redacted]
Assistant United States Attorney
United States Attorney's Office
Eastern District of Virginia
Justin W. Williams United States Attorney's Building
2100 Jamieson Avenue
Alexandria, VA 22314-5794
703-299[redacted]
703-299[redacted] (facsimile)
[redacted]k@usdoj.gov

Attorneys for the United States

By _____
John K. Roche (VSB# 68594)
Perkins Coie, LLP
700 13th St., N.W., Suite 600
Washington, D.C. 20005-3960
Phone: 202-434-1627
Fax: 202-654-9106
JRoche@perkinscoie.com

Attorneys for Google Inc.

FILED

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

2011 JAN 18 P 12:58

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

IN RE 2703(d) ORDER AND 2703(f) PRESERVATION REQUEST RELATING TO GMAIL ACCOUNT [redacted]	Misc. No. 10GJ3793 FILED UNDER SEAL

DECLARATION OF JOHN K. ROCHE IN SUPPORT OF GOOGLE INC.'S MOTION TO MODIFY 2703(d) ORDER FOR PURPOSE OF PROVIDING NOTICE TO USER

I, John K. Roche, declare as follows:

1. I am an attorney licensed to practice in the Commonwealth of Virginia and the District of Columbia, and am admitted to practice before this Court. I am an associate in the law firm of Perkins Coie LLP, counsel of record for Google Inc. ("Google") in this action. As one of the attorneys with responsibility for the representation of Google in this matter, I have personal knowledge of the facts set forth below and am competent to testify about the matters stated herein.

2. Attached hereto as Exhibit 1 is the January 4, 2011 order of this Court issued to Google pursuant to 18 U.S.C. § 2703(d) (the "Order") in the above-referenced matter.

3. Attached hereto as Exhibit 2 is the December 14, 2010 order of this Court issued to Twitter pursuant to 18 U.S.C. § 2703(d) (the "Twitter Order") in the above-referenced matter.

4. Attached hereto as Exhibit 3 is the January 5, 2011 order of this Court unsealing the Twitter Order.

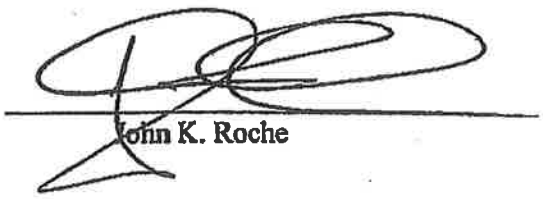
5. Attached hereto as Exhibit 4 is the January 12, 2011 preservation request issued to Google pursuant to 18 U.S.C. § 2703(f) in the above-referenced matter.

6. On January 12, 2011, I spoke with several government attorneys regarding the nondisclosure provisions in the Order. I notified the government that Google wished to

immediately give notice of the Order to its user and requested that the government agree to so modify the Order. The government declined that request saying only that the Order involves a different investigation than the one underlying the Twitter Order. No further explanation was provided. The government offered to release Google from the notice constraint 90 days after it produced, with a provision allowing the government to petition for a further extension. I consequently notified the government that Google intended to file this motion to unseal the Order and to modify its nondisclosure provisions so that Google could give immediate notice to its user. We subsequently agreed on a schedule for filing and argument of this motion.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed this 18th day of January, 2011.



John K. Roche

CERTIFICATE OF SERVICE

I hereby certify that on this 18th day of January, 2011, the foregoing document was sent via hand delivery and email to the following persons:

[redacted]
Assistant United States Attorney
United States Attorney's Office
Eastern District of Virginia
Justin W. Williams United States Attorney's Building
2100 Jamieson Avenue
Alexandria, VA 22314-5794
[redacted] (facsimile)
[redacted]

Attorneys for the United States

By _____
John K. Roche (VSB# 68594)
Perkins Coie, LLP
700 13th St., N.W., Suite 600
Washington, D.C. 20005-3960
Phone: 202-434-1627
Fax: 202-654-9106
JRoche@perkinscoie.com

Attorneys for Google Inc.

EXHIBIT 1

U.S. Department of Justice

United States Attorney

Eastern District of Virginia

Justin W. Williams United States Attorney's Building
2100 Jamieson Avenue
Alexandria, Virginia 22314-5794
(703) 299-3700

FACSIMILE TRANSMISSION COVER PAGE

DATE: 1/5/11

TO: Google, Inc

PHONE: Attn: Custodian of Records

TO FAX NO.: (650) 649-2939 / (650) 249-3429

SENDER: [redacted] Assistant to [redacted]

SENDER'S PHONE NO.: (703) 299 [redacted]

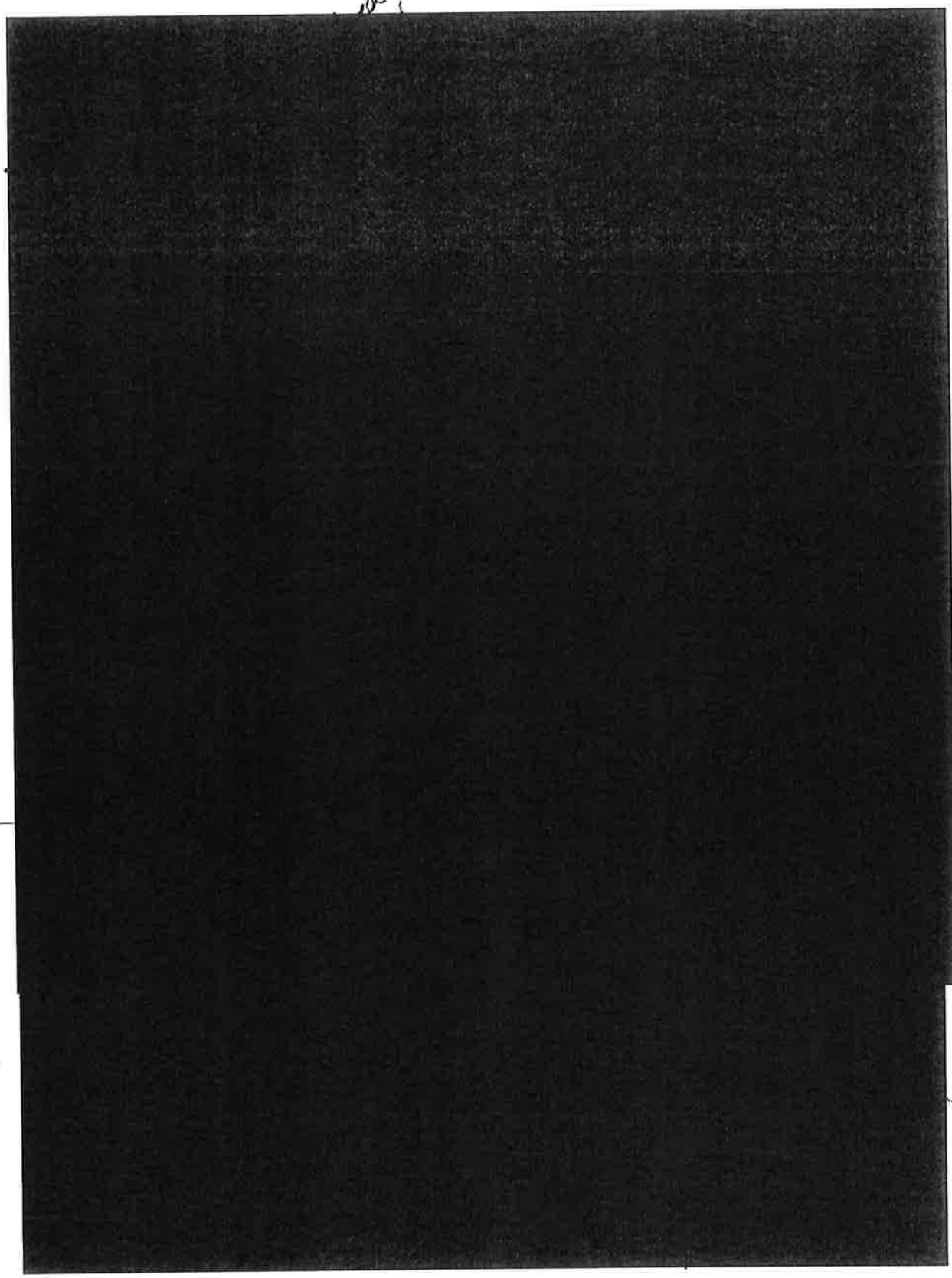
SENDER'S FAX NO.: (703) 299 [redacted]

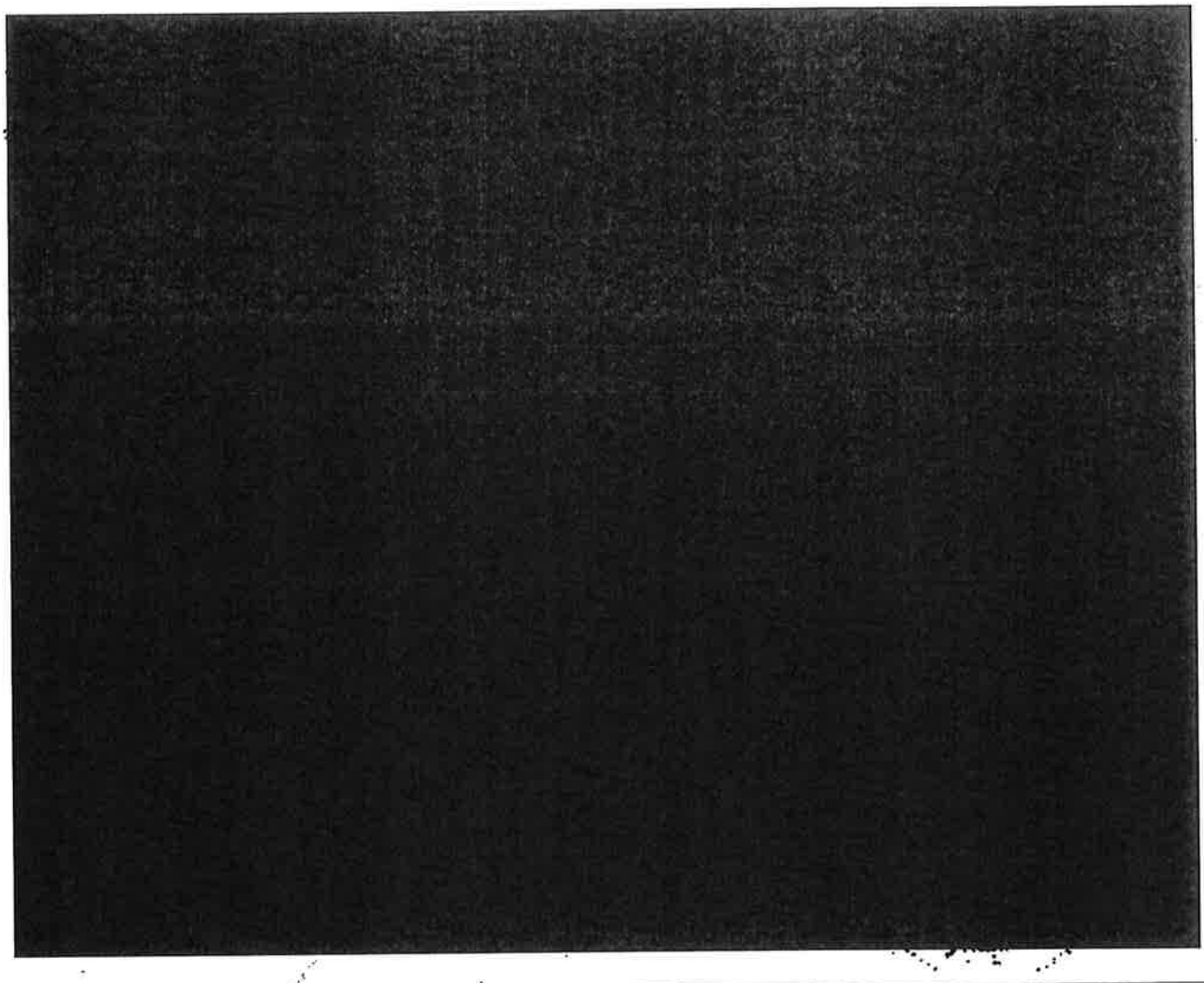
NUMBER OF PAGES: 3 *Not Including Cover Page*

Level of Transmitted Information:

- ☐ **Non-Sensitive Information**
- ☒ **Sensitive But Unclassified (SBU)**
- ☐ **Limited Official Use (LOU)**
- ☐ **Grand Jury Information**
- ☐ **Tax Information**
- ☐ **Law Enforcement Information**
- ☐ **Victim Witness Information**

CONTENTS:





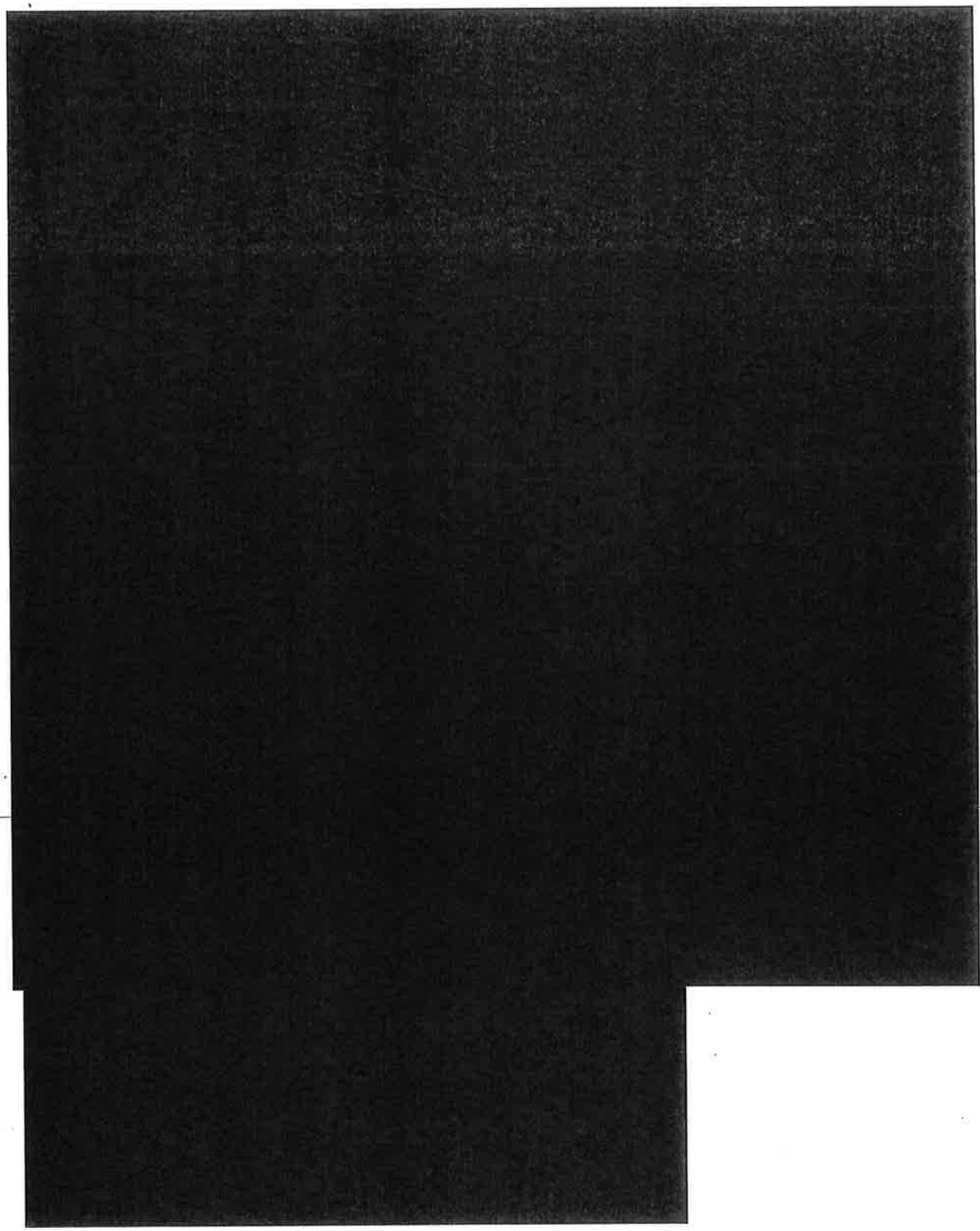


EXHIBIT 2

U.S. Department of Justice

United States Attorney

Eastern District of Virginia

Justin W. Williams United States Attorney's Building
2100 Jamieson Avenue
Alexandria, Virginia 22314-5794
(703) 299-3700

FACSIMILE TRANSMISSION COVER PAGE

DATE: 12/14/10

TO: Twitter Attn: Trust & Safety

PHONE:

TO FAX NO.: (415) 222-9958

SENDER: [redacted] Assistant to [redacted]

SENDER'S PHONE NO.: 703 299 [redacted]

SENDER'S FAX NO.: 703 299 [redacted]

NUMBER OF PAGES: 4 *Not Including Cover Page*

Level of Transmitted Information:

- ☐ **Non-Sensitive Information**
- ☐ **Sensitive But Unclassified (SBU)**
- ☒ **Limited Official Use (LOU)**
- ☐ **Grand Jury Information**
- ☐ **Tax Information**
- ☐ **Law Enforcement Information**
- ☐ **Victim Witness Information**

CONTENTS:

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)	MISC. NO. 10GJ3793
	Filed Under Seal

ORDER

This matter having come before the Court pursuant to an application under Title 18, United States Code, Section 2703, which application requests the issuance of an order under Title 18, United States Code, Section 2703(d) directing Twitter, Inc., an electronic communications service provider and/or a remote computing service, located in San Francisco, California, to disclose certain records and other information, as set forth in Attachment A to this Order, the Court finds that the applicant has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation.

IT APPEARING that the information sought is relevant and material to an ongoing criminal investigation, and that prior notice of this Order to any person of this investigation or this application and Order entered in connection therewith would seriously jeopardize the investigation;

IT IS ORDERED pursuant to Title 18, United States Code, Section 2703(d) that Twitter, Inc. will, within three days of the date of this Order, turn over to the United States the records and other information as set forth in Attachment A to this Order.

IT IS FURTHER ORDERED that the Clerk of the Court shall provide the United States Attorney's Office with three (3) certified copies of this application and Order.

IT IS FURTHER ORDERED that the application and this Order are sealed until otherwise ordered by the Court, and that Twitter shall not disclose the existence of the application or this Order of the Court, or the existence of the investigation, to the listed subscriber or to any other person, unless and until authorized to do so by the Court.

[redacted]
United States Magistrate Judge

12/14/10
Date

ATRUE
CLERK, U.S.
BY DEPUTY CLERK

ATTACHMENT A

You are to provide the following information, if available, preferably as data files on CD-ROM, electronic media, or email [redacted] or otherwise by facsimile to [redacted]

A. The following customer or subscriber account information for each account registered to or associated with [redacted] for the time period November 1, 2009 to present:

1. subscriber names, user names, screen names, or other identities;
2. mailing addresses, residential addresses, business addresses, e-mail addresses, and other contact information;
3. connection records, or records of session times and durations;
4. length of service (including start date) and types of service utilized;
5. telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
6. means and source of payment for such service (including any credit card or bank account number) and billing records.

B. All records and other information relating to the account(s) and time period in Part A, including:

1. records of user activity for any connections made to or from the Account, including the date, time, length, and method of connections, data transfer volume, user name, and source and destination Internet Protocol address(es);
2. non-content information associated with the contents of any communication or file stored by or for the account(s), such as the source and destination email addresses and IP addresses.
3. correspondence and notes of records related to the account(s).

EXHIBIT 3

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE §2703(d) ORDER RELATING TO TWITTER ACCOUNTS: [redacted]	)))))	MISC. NO. 10GJ3793

ORDER TO UNSEAL THE ORDER PURSUANT TO 18 U.S.C. §2703(D)

This matter having come before the Court pursuant to an application under Title 18, United States Code, §2703(d), it appearing that it is in the best interest of the investigation to unseal the Court's Order of December 14, 2010 and authorize Twitter to disclose that Order to its subscribers and customers, it is hereby ORDERED that the above-captioned Order of December 14, 2010 pursuant to 18 U.S.C. §2703(d) be UNSEALED and that Twitter is authorized to disclose such Order. In all other respects, the Court's Order of December 14, 2010 remains in effect.

[redacted]
UNITED STATES MAGISTRATE JUDGE

Date: 1/5/11

Alexandria, Virginia

EXHIBIT 4

FAX TRANSMISSION

United States Attorney
Eastern District of Virginia
Justin W. Williams U.S. Attorney's Office Building
2100 Jamieson Ave.
Alexandria, VA 22314

To	Custodian of Records Google		
Fax	650-649-2939; 650-249-3429		
From	[redacted] Assistant United States Attorney	**Voice**	703-299-3700
Fax	703-299-3781		
Date	January 12, 2011	**Pages**	3, including this page

Subject Preservation letter under 18 U.S.C. sec. 2703(f)

U.S. Department of Justice

United States Attorney
Eastern District of Virginia

Justin W. Williams U.S. Attorney's Office Building
2100 Jamieson Ave.
Alexandria, VA 22314
PHONE: 703-299-3712

January 12, 2011

Google
1600 Amphitheatre Parkway
Mountain View, CA 94043

Attn: Custodian of Records
Facsimile: 650-649-2939; 650-249-3429

Re: Request for Preservation of Records

Dear Google:

Pursuant to Title 18, United States Code, Section 2703(f), this letter is a formal request for the preservation of all stored communications, records, and other evidence in your possession regarding the following email account pending further legal process: [redacted] ("the Account") November 2009 to the present.

I request that you not disclose the existence of this request to the subscriber or any other person, other than as necessary to comply with this request. If compliance with this request might result in a permanent or temporary termination of service to the Account, or otherwise alert any user of the Account as to your actions to preserve the information described below, please contact me as soon as possible and before taking action.

I request that you preserve, for a period of 90 days, the information described below currently in your possession in a form that includes the complete record. This request applies only retrospectively. It does not in any way obligate you to capture and preserve new information that arises after the date of this request. This request applies to the following items, whether in electronic or other form, including information stored on backup media, if available:

1. The contents of any communication or file stored by or for the Account and any associated accounts, and any information associated with those communications or files, such as the source and destination email addresses or IP addresses.

2. All records and other information relating to the Account and any associated accounts including the following:

   a. subscriber names, user names, screen names, or other identities;

b. mailing addresses, residential addresses, business addresses, e-mail addresses, and other contact information;

c. length of service (including start date) and types of service utilized;

d. records of user activity for any connections made to or from the Account, including the date, time, length, and method of connections, data transfer volume, user name, and source and destination Internet Protocol address(es);

e. telephone records, including local and long distance telephone connection records, caller identification records, cellular site and sector information, GPS data, and cellular network identifying information (such as the IMSI, MSISDN, IMEI, MEID, or ESN);

f. telephone or instrument number or other subscriber number or identity, including temporarily assigned network address;

g. means and source of payment for the Account (including any credit card or bank account numbers) and billing records;

h. correspondence and other records of contact by any person or entity about the Account, such as "Help Desk" notes; and

i. any other records or evidence relating to the Account.

If you have questions regarding this request, please call me at 703-299[redacted]

Sincerely,

[redacted]

UNITED STATES ATTORNEY

[redacted]

Assistant United States Attorney

FILED

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

2011 FEB -3 P 3:59

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)	)	MISC. NO. 10GJ3793 11-DM-2
		Filed Under Seal

To: John K. Roche, Esquire
Perkins Coie LLP
700 13th St., N.W., Suite 600
Washington, D.C. 20005-3960
PHONE: 202.434.1627
FAX: 202.654.9106
E-MAIL: JRoche@perkinscoie.com

You are hereby notified that on Wednesday, February 9, 2011, at 11:30 a.m., a hearing will be held before The Honorable Ivan D. Davis, Magistrate Judge on the Fourth Floor at the U.S. District Court, Alexandria, Virginia, on the Government's Motion to Continue Hearing filed on February 3, 2011; and Google, Inc.'s Motion to Modify 2703(d) Order filed on January 18, 2011.

Executed on 2/3/2011

[redacted]
United States Attorney

[redacted]
Assistant United States Attorney
Justin W. Williams U.S. Attorney's Building
2100 Jamieson Avenue
Alexandria, VA 22314
Phone: 703-299-3700
Fax: 703-299-3981

ATTACHMENT B

THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE 2703(d) ORDER AND 2703(f) PRESERVATION REQUEST RELATING TO GMAIL ACCOUNT	Case No. 1:10GJ3793 11-DM-2 **UNDER SEAL**

RESPONSE OF THE UNITED STATES TO GOOGLE'S MOTION TO MODIFY 2703(d) ORDER FOR PURPOSE OF PROVIDING NOTICE TO USER

In its January 18, 2011 motion and supporting memorandum, Google Inc. ("Google") asks this Court to amend its January 4, 2011 order (the "Order") to allow Google to provide immediate notice of the Order to the subscriber of the [redacted] account (the "[redacted] subscriber"), whose records are the subject of the Order. Google also asks that the Order be unsealed; requests permission to discuss the Order with the [redacted] subscriber and his attorneys; and further requests that the [redacted] subscriber be given 20 days from the date of the Court's order to file an appropriate response. For the reasons set forth below, the United States opposes Google's motion and requests that the Court's current order of notice preclusion be maintained and that the Court not permit Google to provide the [redacted] subscriber with immediate notice of the Order. However, as the United States explained to Google on January 12, 2011, the United States does not oppose a modification to the Order that would limit the non-disclosure period to 90 days, with a provision that would allow the government to petition the Court for an additional extension of this period consistent with the requirements of 18 U.S.C. § 2705(b).

Factual & Procedural Background

On January 4, 2011, upon application of the United States pursuant to 18 U.S.C. § 2703(d), this Court issued the Order, requiring Google to disclose certain non-content subscriber and transactional records for the [redacted]ccount. The contents of the subscriber's communications were not required. *See* Roche Decl., Ex. 1. The Order also provided that "the application and this Order are sealed until otherwise ordered by the Court, and that Google shall not disclose the existence of the application or this Order of the Court, or the existence of the investigation, to the listed subscriber or to any other person, unless and until authorized to do so by the Court." *See id.*

Several weeks earlier, on December 14, 2010, Magistrate Judge [redacted] had issued a different order, also pursuant to 18 U.S.C. § 2703(d), that required Twitter, Inc. to disclose similar categories of non-content business records for several Twitter accounts, including a Twitter account under the name [redacted]. *See* Roche Decl., Ex. 2. This order (the "Twitter Order"), like the Order, was issued under seal and contained a non-disclosure provision that prohibited Twitter from disclosing the existence of the application, the Twitter Order, or the existence of the investigation to any person, unless and until authorized to do so by the Court. *See id.* After learning that Twitter would file a motion to modify the Twitter Order so it could disclose it to its customers and subscribers, the government replied that although it was not conceding the merits, it would voluntarily agree to move to unseal the Twitter Order to allow such disclosure.

On January 5, 2011, after finding it was in the best interest of the investigation to permit disclosure to its subscribers and customers, Magistrate Judge [redacted] granted the government's application to unseal the Twitter Order and authorized Twitter to disclose it

("Twitter Unsealing Order"). *See* Roche Decl., Ex. 3. The government sent the Twitter Unsealing Order to counsel for Twitter on January 7, 2011.

On January 12, 2011, counsel for Google asked the government to agree to modify the Order to allow Google to provide immediate notice of the Order to use[redacted] and his legal representative. *See* J. Roche Decl. ¶6. The government did not agree to Google's proposed modification and explained to Google's counsel that the Order presented a different case than the Twitter Order.[1] The government told Google, however, that it would agree to a 90-day limit on the non-disclosure period, subject to a provision that would allow the government to petition for extensions if disclosure would seriously jeopardize the investigation or have an adverse result listed in 18 U.S.C. § 2705. *See* Roche Decl. ¶ 6. Google declined to agree to the government's proposed modification of the Order and instead filed the instant motion on January 18, 2011.

Argument

This Court should not modify its Order to permit Google to provide the[redacted] subscriber with immediate notification or to permit Google to discuss the Order with the[redacted] subscriber and his attorneys. The Order should remain sealed at this time. The Order satisfies all statutory and constitutional requirements, and the[redacted] subscriber would not have a valid basis for challenging it even if Google did provide him with notice. Furthermore, unsealing and permitting disclosure at this time is not in the best interest of the investigation. Unsealing and

[1] The government did not tell counsel for Google that "the Order involve[d] a different investigation than the one underlying the Twitter Order." Roche Decl. ¶ 6; *see also* Google Mot. at 3, 7. Instead, when counsel for Google asked why the government was taking a different position on Google's request to modify the Order than it had taken on Twitter's similar request, the government responded, "It's a different case." This response was intended as a general comment on the different circumstances surrounding the two Orders and was not intended to be an assertion that the Orders related to different investigations.

permitting disclosure of the Twitter Order has already seriously jeopardized the investigation, and the government believes that further disclosures at this time will exacerbate this problem.

I. The Order Was Properly Issued.

A. The Order Is Proper Under 18 U.S.C. § 2705(b).

As this Court has already concluded, the non-disclosure provision of the Order is appropriate under 18 U.S.C. § 2705(b). Under § 2705(b), the government may apply for an order commanding the recipient of a 2703(d) court order – in this case, Google – not to notify any other person of the existence of the order for such period as the court deems appropriate. *See* 18 U.S.C. § 2705(b). The court, in turn, shall issue the requested order "if it determines that there is reason to believe that notification of the existence of the . . . court order 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."

18 U.S.C. § 2705(b). The government's original application, which remains under seal, already provided this Court with reason to believe that notification would have one or more of these adverse results. Based on this information, the Court decided that it was appropriate to include a non-disclosure provision in the Order. *See* Gov't *Ex Parte* Submission, Ex. 1.

The government's application, without more, provided sufficient basis for the Court to conclude that notifying the [redacted] subscriber of the Order will have one or more of the adverse results listed in § 2705(b). The adverse results of disclosing the Twitter Order, including efforts to conceal evidence and harassment (discussed in Part II), further confirm that disclosing the

Order will seriously jeopardize the investigation. Therefore, the non-disclosure provision in the Order is proper under 18 U.S.C. § 2705(b).

B. The Order Is Constitutional.

Google suggests that the Order, which seeks limited subscriber information and transactional records of Google but not the content of the subscriber's communications, "may raise significant free speech and other privilege issues," Google Mot. at 10. But Google does not explain what those issues are. First, Google does not claim that the Order interferes with any First Amendment rights or other privileges that Google may have. *See id.* at 10-11. Second, Google concedes that it "is not properly positioned to [assert First Amendment rights or other privileges] on behalf of users." *Id.* at 10. Third, although Google speculates that the [redacted] subscriber "may wish to assert First Amendment rights . . . or other privileges or defenses to which the user is entitled," *id.* at 10, Google does not identify any specific arguments that the [redacted] subscriber might wish to make, much less assert that the Order is improper under the First Amendment or any other principle of law. *See id.* at 10-11. For the reasons explained below, the Order is proper, and neither the [redacted] subscriber nor Google could mount a viable challenge, First Amendment or otherwise, to the Order.

To begin with, even if the [redacted] subscriber had notice of the Order, he would not be entitled to bring a wide-ranging motion to vacate it. Although the Stored Communications Act (18 U.S.C. §§ 2701-12) does authorize some judicial remedies for subscribers who seek to challenge orders, *see* 18 U.S.C. § 2704(b), these remedies apply to legal process seeking the *content* of the subscriber's communications and do not apply to legal process for business

records under 18 U.S.C. § 2703(d), like the Order here.[2] Instead, § 2703(d) provides remedies only for service providers, and only then if "the 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 Stored Communications Act provides that the "remedies and sanctions described in [the Act] are the only judicial remedies and sanctions for nonconstitutional violations of [the Act]." Thus, Congress did not provide wide ranging remedies that would allow subscribers, such as [redacted], to challenge non-content orders, such as the Order here.[3]

Even if the subscriber had standing and wished to assert a First Amendment challenge, it would be meritless. As the Supreme Court has recognized, "neither the First Amendment nor any other constitutional provision protects the average citizen from disclosing to a grand jury information that he has received in confidence."[4] *Branzburg v. Hayes*, 408 U.S. 665, 682

---

[2] Even if the [redacted] subscriber could use the "customer challenge" procedures in § 2704(b) to bring a motion to vacate, he would have to convince the Court that there is no "reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry." 18 U.S.C. § 2704(b)(4). The [redacted] subscriber cannot meet this standard – the Court has already found that "records or other information sought are relevant and material to an ongoing criminal investigation." *See* Roche Decl., Ex. 1.

[3] Congress's intent that subscribers could challenge legal process seeking the content of their communications, but not legal process seeking business records, is confirmed by reading the Stored Communications Act as a whole. Section 2703 sets forth the legal process required to obtain non-content business records. It expressly provides that subscribers are not even entitled to notice that the government obtained their information. *See* 18 U.S.C. § 2703(c)(3). Section 2703(b), on the other hand, sets forth the legal process required to obtain contents of communications. It expressly provides that notice to subscribers (albeit notice that may be delayed) is required for legal process unless a search warrant is obtained.

[4] Most cases that evaluate First Amendment challenges to the compelled disclosure of documents involve subpoenas, rather than court orders. Court orders issued under 18 U.S.C. § 2703(d), like the Order, are similar to subpoenas because they also require the disclosure of documents, but they are arguably more protective of citizens' interests because they are subject to prior judicial review and require a higher factual showing for issuance. *See* 18 U.S.C. § 2703(d). Accordingly, a party who challenges a § 2703(d) court order should be subjected to standards that are at least as stringent as those applied to a motion to quash a subpoena.

(1972). This is true even if the [redacted] subscriber is "a journalist or engaged in other constitutionally protected activities."[5] Google Mot. at 10. As the Supreme Court has concluded, "the Constitution does not . . . exempt the newsman from performing the citizen's normal duty of appearing and furnishing information relevant to the grand jury's task." *Id.* at 691. Indeed, journalists have no special privilege to resist compelled disclosure of their records, absent evidence that the government is acting in bad faith. *See In re Shain*, 978 F.2d 850, 852 (4th Cir. 1992); *Univ. of Pennsylvania v. E.E.O.C.*, 493 U.S. 182, 201 n.8 (1990) (implying that "the bad-faith exercise of grand jury powers" is the only basis for a First Amendment challenge to a subpoena).

In this case, even if the [redacted] subscriber were to bring a First Amendment challenge, he could not quash the Order because he could not show that the government has acted in bad faith, either in conducting its criminal investigation or in obtaining the Order. The government described the nature of its investigation in its application for the Order, and the Court had an opportunity to review the legitimacy of the investigation before deciding to issue the Order. The government's decision to pursue the records described in the Order was also subject to judicial review by this Court, which concluded that it was proper to issue the Order because the government "offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation." Roche Decl., Ex. 1; *see also* 18 U.S.C. § 2703(d). The government has acted in good faith throughout this criminal investigation, and there is no evidence that either the investigation or the Order is intended to harass the [redacted] subscriber or anyone else. *See United States v. Steelhammer*, 539 F.2d 373, 376 (4th Cir. 1976) (Winter, J., dissenting), *adopted by the*

[5] The government does not concede that the [redacted] subscriber is a journalist.

court en banc, 561 F.2d 539, 540 (4th Cir. 1977) ("[T]he record fails to turn up even a scintilla of evidence that the reporters were subpoenaed to harass them or to embarrass their newsgathering abilities . . ."). Accordingly, even if the Order required the [redacted] subscriber to disclose his Google records himself, th[redacted] subscriber would not have a colorable First Amendment argument for quashing the Order.

The [redacted] subscriber's potential challenges to the Order are even weaker because of the Order's limited scope. The Order requires Google to disclose certain of its business records about the [redacted] subscriber account, but it does not seek the content of any communication, attempt to control or direct the content of the [redacted] subscriber's speech, or impose direct burdens on any journalistic or academic activities in which the [redacted] subscriber may be engaging. *See* Roche Decl., Ex. 1; *Branzburg*, 408 U.S. at 691 (requiring reporter to comply with subpoena "involves no restraint on what newspapers may publish, or on the type or quality of information reporters may seek to acquire," nor does it threaten "a large number or percentage of all confidential news sources"); *Univ. of Pennsylvania*, 493 U.S. at 197-98 (subpoena for academic papers does not impose a content-based or direct burden on university).

Indeed, the Order simply requires disclosure of "non-content" information, such as the [redacted] subscriber's name and address, the IP addresses associated with the [redacted] subscriber's logins to the account, and the email addresses of those with whom the subscriber has corresponded. *See* Roche Decl., Ex. 1; 18 U.S.C. § 2703(c). The [redacted] subscriber has no Fourth Amendment privacy interest in any of this information and therefore could not successfully challenge the Order under the Fourth Amendment, any more than he could challenge it under the First Amendment. *See, e.g.*, *United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010) (IP addresses); *United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008)

(subscriber information); *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) (source or destination addresses of email).

As discussed above, even if the [redacted] subscriber had standing to challenge the Order, he has no viable arguments for quashing the Order. Google implies, however, that the potential merit of a subscriber's arguments is irrelevant, and that subscribers have some inherent right to be notified when their records are obtained under § 2703 so that the subscribers "may decide whether to object" to the disclosure. Google Mot. at 11. This assertion is contrary to the plain language of § 2703, pursuant to which subscribers are not entitled to notice when the government obtains their records and information pursuant to § 2703(c). *See* 18 U.S.C. § 2703(c)(3) ("A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer."); *In re Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 620 F.3d 304, 307 (3d Cir. 2010); *In re Application of the United States for an Order Pursuant to 18 U.S.C. 2703(d)*, 36 F. Supp. 2d 430, 432 (D. Mass. 1999). As further discussed above, the Order was issued under § 2703(c) because it seeks only records and other information pertaining to the [redacted] subscriber, not including the contents of communications. *See* Roche Decl., Ex. 1; 18 U.S.C. §§ 2703(c)(1)(B) and (c)(2) (authorizing government to use a court order under § 2703(d) to obtain the records described in the Order). Accordingly, the [redacted] subscriber is not entitled to notice of the Order from the government, from Google, or from anyone else. *See S.E.C. v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984) ("[Prior Supreme Court] rulings disable respondents from arguing that notice of subpoenas issued to third parties is necessary to allow a target to prevent an unconstitutional search or seizure of his papers.").

Moreover, Google's failure to directly assert its own First Amendment rights in its motion is with good cause: Google has no viable First Amendment argument to make on its own behalf. Courts regularly issue sealing orders, protective orders, and other non-disclosure orders that preclude private parties from discussing matters before the court. *See e.g., In re Application of United States of America for an Order Pursuant to 18 U.S.C. § 2703(d) Directed to Cablevision Systems Corp.*, 158 F.Supp.2d 644, 648-49 (D.Md. 2001) (holding that the Electronic Communications Privacy Act implicitly repealed provisions of the Cable Communications Policy Act that required notice to a subscriber of a cable company service of a court order directing disclosure of the subscriber's personal information) (citing in support, 12 U.S.C. § 3409 (authorizing delayed notice for financial institutions); 18 U.S.C. §§ 2511(2)(a)(ii) (prohibiting disclosure of wire interceptions); § 3123(d) (prohibiting disclosure of pen registers or trap and trace devices)).

Indeed, 18 U.S.C. § 2705(b) was enacted almost twenty-five years ago, and to the government's knowledge, no court has ever held that its procedures fail to comply with the requirements of the First Amendment. *See* Electronic Communications Privacy Act of 1986, PL 99-508, § 201, 100 Stat. 1848 (1986). Furthermore, the government has already told Google that it will agree to seek modification of the Order to limit the non-disclosure period to 90 days, subject to possible court-ordered extensions, *see* Roche Decl. ¶ 6. This cures Google's complaint that the current Order has a "perpetual" or "indefinite" period of non-disclosure. Google Mot. at 2, 7, 8. Accordingly, even if Google had challenged the non-disclosure provision based on its own First Amendment rights, this challenge would have failed.

For all of the reasons set forth above, the Order, including its non-disclosure and sealing requirements, is proper in every respect, including under the First and Fourth Amendments, and

the government does not oppose limiting the duration of the non-disclosure period to 90 days, subject to possible extensions consistent with the requirements of 18 U.S.C. § 2705(b).

II. The Disclosure of the Twitter Order Does Not Justify Disclosure of This Order, Particularly When Unsealing the Twitter Order Already has Seriously Jeopardized the Investigation

Google argues that because the government voluntarily unsealed and allowed disclosure of the Twitter Order, the Court should do so here, particularly because both orders are part of the WikiLeaks investigation, the existence of which has been publicly acknowledged. *See* Google Mot. at 1, 2. Google is wrong. The government's voluntary decision to move to lift the notice preclusion aspect of the Twitter Order based upon its particularized assessment of the continuing need for that preclusion was a reasonable exercise of its prosecutorial discretion. This previous decision should not bind the government as to other orders. Moreover, the unsealing and disclosure of the Twitter Order already has seriously jeopardized the investigation even though the existence of the investigation had been publicly acknowledged. Unsealing and allowing disclosure by Google will exacerbate the harm. Indeed, in light of the events that followed the unsealing and disclosure of the Twitter Order, had the government known then what it does now, it would not have voluntarily filed the motion to authorize it.

The Twitter Unsealing Order was premised on the Court's finding that at that time, allowing disclosure of that order to Twitter's customers and subscribers served the best interest of the case. *See* Roche Decl. Ex. 3. The decision to move the Court to unseal the order was based on the government's assessment of the continuing need for notice preclusion for the Twitter Order, including its estimation of the importance of the information sought to the investigation, the resources that might be required to defend that order, and the expected consequences of allowing disclosure. The decision was not based on a belief that the § 2705(b)

non-disclosure order and sealing were no longer legally justified. The government did not concede the merits of Twitter's planned motion. At this time, the government has not voluntarily moved to modify the valid Google Order because it believes that disclosure and unsealing will not serve the best interest of the case. So long as non-disclosure and sealing remain justified under the standards set out by law, as it does here, a decision such as this falls squarely within the government's prosecutorial discretion, involving not only factors and considerations relevant to the conduct of the ongoing criminal investigation that are ill-suited to judicial review, but also theories protected by the attorney work product doctrine. *See generally, Ex Parte Submission*; *Reno v. American-Arab Anti-Discrimination Comm.*, 525 U.S. 471, 490 (1999) (quoting *Wayte v. United States,* 470 U.S. 598, 607-608 (1985)) (issues that fall within the scope of prosecutorial discretion are "particularly ill-suited to judicial review"); *see also United States v. Juvenile Male,* 2010 WL 5158562 (4th Cir. 2010) (unpublished) ("The Government's certification that a substantial federal interest exists is generally regarded as a matter of prosecutorial discretion, and while this decision is not immune from judicial review, we accord the decision substantial deference.") (citing *United States v. Juvenile Male # 1,* 86 F.3d 1314, 1319 (4th Cir.1996)); *Hickman v. Taylor,* 329 U.S. 495, 510-511 (1947) (attorney work product covers legal theories and strategy).

In any event, the government's decision to move to lift the notice preclusion aspect of the Twitter Order should neither bind its decisions with respect to the Order, nor should its decision be used against it. Either result would discourage particularized analysis of the need for notice preclusion and would also punish voluntary disclosure by the government, contrary to established public policy favoring those results. *Cf.* Fed.R.Evid. 408 advisory committee's notes

("As a matter of general agreement, evidence of an offer to compromise a claim is not receivable in evidence as an admission of, as the case may be, the validity or invalidity of the claim.").

Moreover, circumstances have changed in the investigation since – and in part as a result of – the government's decision to unseal and disclose the Twitter Order, demonstrating why this Order presents a different case. Specifically, the government failed to anticipate the degree of damage that would be caused by the unsealing and disclosure of the Twitter Order:

(1) On January 7, 2011, the same day the government sent the Unsealing Order to Twitter's counsel, a copy of the Twitter Order, including the judge's name, prosecutor's email address, and the fax cover sheet, identifying the names of the prosecutor and a legal assistant and the legal assistant's telephone number, were posted on the Internet at http://mobile.salon.com/opinion/greenwald/2011/01/07/twitter/index.html; *See* Gov't Ex. 1.

(2) One reason for sealing and ordering non-disclosure under Section 2705 in the Twitter case, as well as here, is that disclosure would seriously jeopardize the investigation because it might cause suspects to change their patterns of behaviour, notify confederates or flee. Once the Twitter Order was unsealed, the Twitter account holder with the username [redacted] announced a change in his behavior and made a general announcement to others who might potentially have evidence relevant to the investigation by posting a message to Twitter on January 7, 2011, that stated "Do not send me Direct Messages – My Twitter account contents have apparently been invited to the (presumably Grand Jury) in Alexandria." *See* Gov't Ex. 2

(3) Thus, despite the general, public knowledge of the WikiLeaks investigation, [redacted] apparently continued to use his Twitter account to receive Direct Messages until he had

actual knowledge of the specific investigative steps taken to obtain transactional records from that account. This confirms the government's representations in its current application for non-disclosure and indicates that the user might be willing to destroy evidence or otherwise try to disrupt the ongoing investigation.

(4) Because of the disclosure of the Twitter Order, a public campaign commenced, pressuring providers to challenge non-disclosure orders to disclose compulsory process. On January 8, 2011, the Twitter account of [redacted] tweeted, "Note that we can assume Google & Facebook also have secret U.S. government subpoenas. They make no comment. Did they fold?" *See* Gov't Ex. 3. On January 10, 2011, the Twitter account of [redacted] posted, "This matter does beg the question who else has gotten such court orders and whether other parties have silently complied with such orders. Hello Facebook? Google?" *See* Gov't Ex. 4; *see also* Wikipedia, "Twitter subpoena," http://en.wikipedia.org/wiki/Twitter_subpoena, Gov't Ex. 5; P. Beaumont, guardian.co.uk, [redacted] *Demands Google and Facebook Unseal Subpoenas,* January 8, 2011, http://www.guardian.co.uk/media/2011/jan/08/[redacted]-calls-google-facebook-us-subpoenas; http://techland.time.com/2011/01/14/twitter-[redacted]-and-the-broken-market-for-consumer-privacy/ ("The tech world is abuzz with a remarkable display of backbone by Twitter in the [redacted] case. It deserves wider notice" . . . "Twitter stalled, fighting and winning a motion to lift the gag order, which is how we know about the case. (If the judge had believed government claims that lifting the gag would blow the investigation, she could equally have rejected Twitter's motion.) Having obtained permission, Twitter notified its users and promised to hand over nothing if they filed a motion to quash within ten days. That is simply the gold standard of customer protection,

enabling courts to balance the legitimate needs of prosecutors with the civil liberties of their targets. It almost never happens.");

http://www.wired.com/threatlevel/2011/01/twitter/# ("ANALYSIS: Twitter introduced a new feature last month without telling anyone about it, and the rest of the tech world should take note and come up with its own version of it. Twitter beta-tested a spine.");

http://www.fastcompany.com/1716100/why-twitter-was-the-only-company-to-challenge-the-secret-[redacted]-subpoena.

(5) Because the Twitter Order was posted on the Internet, without redaction, an employee at the U.S. Attorney's Office was subjected to harassment over the Internet, including the posting of her home address, and email messages, including the attached, *see* Gov't Ex. 6. Time and resources were diverted from the continued investigation to increasing security measures for prosecutors. This harassment may also make all government witnesses reluctant to testify fully in the future, for fear of similar retribution.

Thus, the disclosure and unsealing of the Twitter Order has seriously jeopardized the investigation – candidly, much more than the government anticipated at the time it made its decision to move to lift the notice preclusion aspect of the Twitter Order. Among other things, the government confirmed that despite the public nature of the investigation, disclosure of the particular investigative step at issue in the Twitter Order increased the risk that witnesses and targets would tamper with or destroy evidence in relevant Twitter accounts, including by altering their modes of communication to evade future investigative efforts.

The disclosure and unsealing also presented the unforeseen risk of witness intimidation. Protecting witnesses from public exposure encourages them to voluntarily come forward and to testify fully without fear of retribution. These two core principles underlie the need for secrecy

in the grand jury process. *See United States v. Reiner*, 934 F.Supp. 721, 723 (E.D.Va. 1996) (citing *Douglas Oil Co. v. Petrol Stops Northwest*, 441 U.S. 211, 219 (1979)). Unfortunately, there are already indications that disclosure of the Twitter Order has encouraged providers – who are also potential witnesses – to resist the government's attempts to gather relevant user information. The government is aware of at least one other potential challenge by a provider to the non-disclosure provision and sealing of another 2703(d) Order in this case because of the fall-out from the unsealing and disclosure of the Twitter Order. More can reasonably be expected. Providers may fear that public exposure of their willing compliance with court orders will hurt their reputation and therefore feel pressure to challenge non-disclosure orders. At the same time, repeatedly unsealing and disclosing process during an ongoing investigation presents a heightened risk of jeopardizing the investigation, potentially revealing each step the government has taken and highlighting those that have yet to be taken. This would provide a detailed investigative roadmap to targets and witnesses and make it easier to destroy evidence and change patterns of behavior to avoid detection.

Finally, the disclosure and unsealing of the Twitter Order has already resulted in harassment that disrupted the investigation by diverting resources and attention, as demonstrated above. A similar reaction can be expected if disclosure and unsealing is authorized here. For all of these reasons, the government has not agreed to disclosure of the Order. The non-disclosure and sealing provisions of the Order remain legally justified, and disclosure is not in the best interest of the investigation.[6] To the contrary, if the government knew on January 4, 2011 what it does now, it would not have moved to unseal and authorize disclosure of the Twitter Order.

[6] In this case, the government has offered to self-impose a 90 day limit on sealing, with the ability to petition the court to extend as needed.

Conclusion

In conclusion, the court should deny Google's motion to modify the Order. The Order, including the provisions that order sealing and non-disclosure by Google, remain warranted more than ever. Unsealing and disclosure of the Order would significantly jeopardize the investigation.

Respectfully Submitted,

[redacted]
United States Attorney

By: [redacted]
Assistant United States Attorney

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing pleading was delivered on this 28th day of January 2011 to the Clerk's Office and that service will be made on the following individuals by electronic mail and otherwise:

John K. Roche, Esquire
Perkins Coie LLP
700 13th St., N.W., Suite 600
Washington, D.C. 20005-3960
PHONE: 202.434.1627
FAX: 202.654.9106
E-MAIL: JRoche@perkinscoie.com

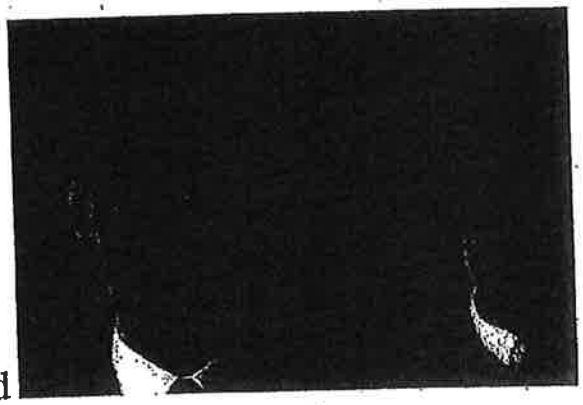
[redacted]
Assistant United States Attorney

GOVERNMENT EXHIBIT 1

Fri, 07 Jan 2011 17:08:00 ET

DOJ subpoenas Twitter records of several [redacted] volunteers

A federal court authorizes the DOJ to demand sweeping information about the accounts of several [redacted] volunteer



By Glenn Greenwald
AP
U.S. Attorney General Eric Holder.

- Blog:
  - Glenn Greenwald
- Topics:
  - WikiLeaks

(updated below - Update II - Update III)

Last night, [redacted] -- a former [redacted] volunteer and current member of the [redacted] Parliament -- announced (on Twitter) that she had been notified by Twitter that the DOJ had served a Subpoena demanding information "about all my tweets and more since November 1st 2009." Several news outlets, including *The Guardian*, wrote about [redacted] announcement.

What hasn't been reported is that the Subpoena served on Twitter -- which is actually an Order from a federal court that the DOJ requested -- seeks the same information for numerous other individuals currently or formerly associated with [redacted] including [redacted] and [redacted] It also seeks the same information for [redacted] and for [redacted] Twitter account.

The information demanded by the DOJ is sweeping in scope. It includes all mailing addresses and billing information known for the user, all connection records and session times, all IP addresses used to access Twitter, all known email accounts, as well as the "means and source of payment," including banking records and credit cards. It seeks all of that information for the period beginning November 1, 2009, through the present. A copy of the Order served on Twitter, obtained exclusively by *Salon*, is here.

The Order was signed by a federal Magistrate Judge in the Eastern District of Virginia, [redacted], and served on Twitter by the DOJ division for that district. It states that there is "reasonable ground to believe that the records or other information sought are relevant and material to an ongoing criminal investigation," the language required by the relevant statute. It was issued on December 14 and ordered sealed -- i.e., kept secret from the targets of the Order. It gave Twitter three days to respond and barred the company from notifying anyone, including the users, of the existence of the Order. On January 5, the same judge directed that the Order be unsealed at Twitter's request in order to inform the users and give them 10 days to object; had Twitter not so requested, it would have been compelled to turn over this information without the knowledge of its users. A copy of the unsealing order is here.

[redacted] told me that as "a member of the Foreign Affairs Committee [of Iceland's Parliament] and the NATO parliamentary assembly," she intends to "call for a meeting at the Committee early next week and ask for the ambassador to meet" her to protest the DOJ's subpoena for her records. The other individuals named in the subpoena were unwilling to publicly comment until speaking with their lawyer.

I'll have much more on the implications of this tomorrow. Suffice to say, this is a serious escalation of the DOJ's efforts to probe, harass and intimidate anyone having to do with [redacted] Previously, [redacted] as well as [redacted] supporter [redacted] -- both American citizens -- had their laptops and other electronic equipment seized at the border by Homeland Security agents when attempting to re-enter the U.S.

UPDATE: Three other points: first, the three named producers of the "Collateral Murder" video -- depicting and commenting on the U.S. Apache helicopter attack on journalists and civilians in Baghdad -- were [redacted], and [redacted] (whose name is misspelled in the DOJ's documents). Since [redacted] has had no connection to WikiLeaks for several months and [redacted]'s association has diminished substantially over time, it seems clear that they were selected due to their involvement in the release of that film. Second, the unsealing order does not name either [redacted] which means either that Twitter did not request permission to notify them of the Subpoena or that they did request it but the court denied it (then again, neither "[redacted]" are names of Twitter accounts, and the company has no way of knowing with certainty which accounts are theirs, so perhaps Twitter only sought an unsealing order for actual Twitter accounts named in the Order). Finally, [redacted] and [redacted] intend to contest this Order.

UPDATE II: It's worth recalling -- and I hope journalists writing about this story remind themselves -- that all of this extraordinary probing and "criminal" investigating is stemming from WikiLeaks' doing nothing more than publishing classified information showing what the U.S. Government is doing: something investigative journalists, by definition, do all the time.

And the key question now is this: did other Internet and social network companies (Google, Facebook, etc.) receive similar Orders and then quietly comply? It's difficult to imagine why the DOJ would want information only from Twitter; if anything, given the limited information it has about users, Twitter would seem one of the least fruitful avenues to pursue. But if other companies did receive and quietly comply with these orders, it will be a long time before we know, if we ever do, given the prohibition in these orders on disclosing even its existence to anyone.

UPDATE III: [redacted] Interior Minister, Ögmundur Jónasson, described the DOJ's efforts to obtain the Twitter information of a [redacted] as "grave and odd." While suggesting some criticisms of [redacted], he added: "if we manage to make government transparent and give all of us **some insight into what is happening in countries involved in warfare it can only be for the good.**" The DOJ's investigation of a [redacted] -- as part of an effort to intimidate anyone supporting [redacted] and to criminalize journalism that exposes what the U.S. Government does -- is one of the most extreme acts yet in the Obama administration's always-escalating war on whistleblowers, and shows how just excessive and paranoid the administration is when it comes to transparency: all this from a President who ran on a vow to have the "most transparent administration in history" and to "Protect Whistleblowers."

U.S. Department of Justice

United States Attorney

Eastern District of Virginia

Justin W. Williams United States Attorney's Building
2100 Jamieson Avenue
Alexandria, Virginia 22314-5794
(703) 299-3700

FACSIMILE TRANSMISSION COVER PAGE

DATE: 12/14/10

TO: Twitter Attn: Trust & Safety

PHONE:

TO FAX NO.: (415) 222-9958

SENDER: [redacted], Assistant to [redacted]

SENDER'S PHONE NO.: 703 [redacted]

SENDER'S FAX NO.: 703 [redacted]

NUMBER OF PAGES: 4 *Not Including Cover Page*

Level of Transmitted Information:

- ☐ **Non-Sensitive Information**
- ☐ **Sensitive But Unclassified (SBU)**
- ☒ **Limited Official Use (LOU)**
- ☐ **Grand Jury Information**
- ☐ **Tax Information**
- ☐ **Law Enforcement Information**
- ☐ **Victim Witness Information**

CONTENTS:

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)	MISC. NO. 10GJ3793
	Filed Under Seal

ORDER

This matter having come before the Court pursuant to an application under Title 18, United States Code, Section 2703, which application requests the issuance of an order under Title 18, United States Code, Section 2703(d) directing Twitter, Inc., an electronic communications service provider and/or a remote computing service, located in San Francisco, California, to disclose certain records and other information, as set forth in Attachment A to this Order, the Court finds that the applicant has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation.

IT APPEARING that the information sought is relevant and material to an ongoing criminal investigation, and that prior notice of this Order to any person of this investigation or this application and Order entered in connection therewith would seriously jeopardize the investigation;

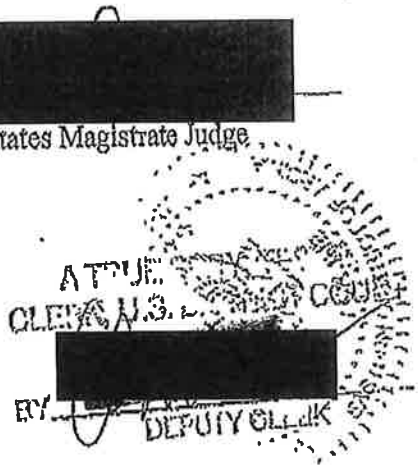
IT IS ORDERED pursuant to Title 18, United States Code, Section 2703(d) that Twitter, Inc. will, within three days of the date of this Order, turn over to the United States the records and other information as set forth in Attachment A to this Order.

IT IS FURTHER ORDERED that the Clerk of the Court shall provide the United States Attorney's Office with three (3) certified copies of this application and Order.

IT IS FURTHER ORDERED that the application and this Order are sealed until otherwise ordered by the Court, and that Twitter shall not disclose the existence of the application or this Order of the Court, or the existence of the investigation, to the listed subscriber or to any other person, unless and until authorized to do so by the Court.

[redacted]
United States Magistrate Judge

12/14/10
Date



ATTACHMENT A

You are to provide the following information, if available, preferably as data files on CD-ROM, electronic media, or email [redacted] or otherwise by facsimile to [redacted]

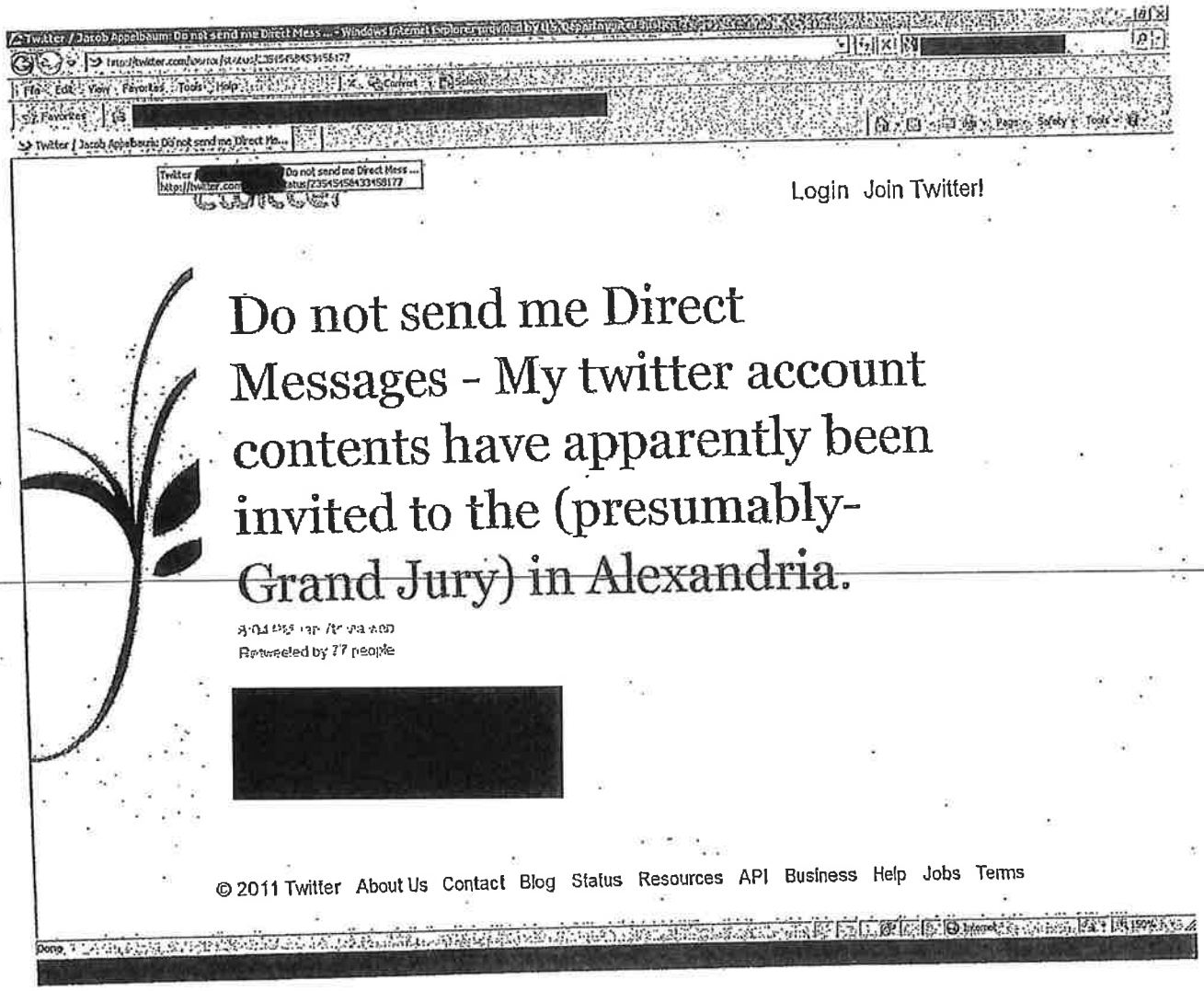
A. The following customer or subscriber account information for each account registered to or associated with [redacted] for the time period November 1, 2009 to present:

1. subscriber names, user names, screen names, or other identities;
2. mailing addresses, residential addresses, business addresses, e-mail addresses, and other contact information;
3. connection records, or records of session times and durations;
4. length of service (including start date) and types of service utilized;
5. telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
6. means and source of payment for such service (including any credit card or bank account number) and billing records.

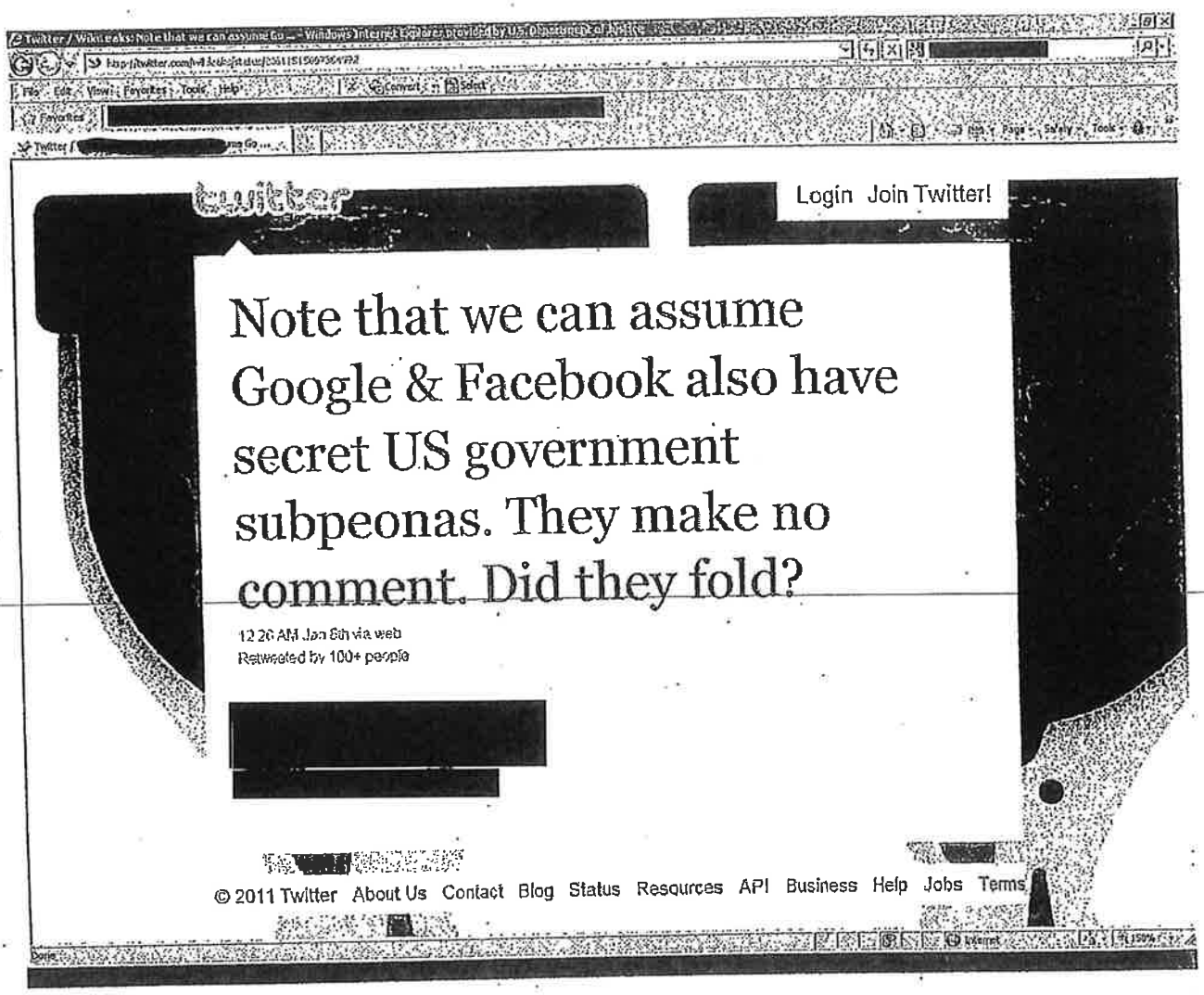
B. All records and other information relating to the account(s) and time period in Part A, including:

1. records of user activity for any connections made to or from the Account, including the date, time, length, and method of connections, data transfer volume, user name, and source and destination Internet Protocol address(es);
2. non-content information associated with the contents of any communication or file stored by or for the account(s), such as the source and destination email addresses and IP addresses.
3. correspondence and notes of records related to the account(s).

GOVERNMENT EXHIBIT 2


Twitter / Jacob Appelbaum: Do not send me Direct Mess ... - Windows Internet Explorer provided by
Favorites
Twitter / Jacob Appelbaum: Do not send me Direct Me...
Do not send me Direct Mess ...
Login Join Twitter!
Do not send me Direct Messages - My twitter account contents have apparently been invited to the (presumably-Grand Jury) in Alexandria.
Retweeted by 77 people
© 2011 Twitter About Us Contact Blog Status Resources API Business Help Jobs Terms
Done

GOVERNMENT EXHIBIT 3


Twitter / Wikileaks: Note that we can assume Go... - Windows Internet Explorer provided by US Department of Justice
Favorites
Twitter
Login Join Twitter!
Note that we can assume Google & Facebook also have secret US government subpeonas. They make no comment. Did they fold?
12:20 AM Jan 5th via web
Retweeted by 100+ people
[redacted]
© 2011 Twitter About Us Contact Blog Status Resources API Business Help Jobs Terms
Done
Internet

GOVERNMENT EXHIBIT 4

trying to save the wounded, and you wake up the next day a nefarious left-wing terror activist-adjudant secretly spending millions on web hosting. I wonder what I'll be tomorrow.

January 12th, 2011 - 02:07 | 41 comments
Please share: [redacted]

On the Twitter court order

Dear journalists,

Yet again I am being inundated with your e-mails, text messages, phone calls and unannounced house visits. (The latter is new, unwelcome and the fastest way to get a non-expiring entry on my media blacklist.)

I could easily spend all my time answering the same questions with the same answers instead of taking some time to think for myself. This is not your fault. I can see there's a story here and you need to cover it. I just hope you'll forgive me for writing down my thoughts just once on this blog. I realize you may "just have a few questions" or desperately need my voice or footage of my talking head, but I'll most likely still point you to this text. It's nothing personal.

What happened?

On December 14 of 2010, the US Department of Justice has had a court order issued to force Twitter to send them various bits of information regarding my Twitter account as well as of the twitter accounts of [redacted]. In my previous blog post, I have erroneously referred to this order as a subpoena, which it isn't. I'm not a US lawyer, but some apparently profound thoughts about various aspects of this order can be found here.

I found out about the order because Twitter did the right thing and successfully fought for a second court order so they were able to tell us. The e-mail from twitter also says we have ten days to announce that we're fighting this in court or otherwise they'll give the DOJ the requested information. I'll write more about Twitter's role soon.

Apparently someone thinks that whatever records Twitter has regarding my account are "relevant and material to an ongoing criminal investigation". It is not clear from the documents that have presently been made public what my role in this apparent investigation is.

So what does Twitter have on me?

Basically my tweets, which are publicly accessible, and the IP-numbers I connected from. I don't use Twitter all that much and for convenience my tweets are generally posted through a plugin on this blog. I have never sent or received private messages on twitter. In other words: what Twitter has on me is unspectacular.

This matter does beg the question who else has gotten such court orders and whether other parties have silently complied with such orders. Hello Facebook? Google?

Why did this happen?

I don't know. But from the list of names we can speculate this has something to do with the release of the "Collateral Murder" video in april of 2010. That video, shot from a US helicopter over Baghdad, shows the shooting of a Reuters photographer and subsequently of the civilians that try to rescue him. I travelled to Iceland to help out with the preparations for disseminating this video. I feel, probably like most people that saw the video, that showing that video served the important purpose of shining light on the hidden realities of present-day war.

The entire process of releasing this video is ridiculously well-documented as Raffi Khatchadourian, a journalist for The New Yorker, was with us the whole time. I recommend his article for an in-depth look at what happened. For a broader look at my life over the past year or so, I recommend reading a keynote speech I delivered in Berlin a few weeks ago.

So what am I going to do now?

Being involved in a criminal investigation, and especially one which is likely to have huge political pressure behind it, is a very serious matter. So I am talking to lawyers, trying to better understand what is going on and I am weighing my options. Frequent readers of this blog will likely be the first to know if I have something new to say.

January 10th, 2011 - 00:41 | 109 comments
Please share: [redacted]

US DOJ wants my twitter account info

It's a warm and fuzzy feeling to know that somewhere, far away, people are thinking about you. Last night I received this rather interesting e-mail from twitter:

> Kessel, Jan-07 11:20 am (PST):
> Dear Twitter User:
>
> We are writing to inform you that Twitter has received legal process requesting information regarding your Twitter account[redacted]. A copy of the legal process is attached. The legal process requires Twitter to produce documents related to your account.
>
> Please be advised that Twitter will respond to this request in 10 days from the date of this notice unless we receive notice from you that a motion to quash the legal process has been filed or that this matter has been otherwise resolved.
>
> To respond to this notice, please e-mail us at <removed>.
>
> This notice is not legal advice. You may wish to consult legal counsel about this matter. If you need assistance seeking counsel, you may consider contacting the Electronic Frontier Foundation <contact info removed> or the ACLU <contact info removed>.

GOVERNMENT EXHIBIT 5

Twitter subpoena

From Wikipedia, the free encyclopedia

On 14 December 2010 the United States Department of Justice issued a subpoena accompanied by a national security letter to Twitter in relation to ongoing investigations of [redacted].[1][2] While only five people were individually named, according to lawyer Mark Stephens the order effectively entailed the collection in relation to criminal prosecution of the personal identifying information of over six hundred thousand Twitter users, namely those who were "followers" of [redacted].[3][1][2][4] Twitter appealed against the accompanying so-called gag order in order to be able to disclose its existence to its users, and was ultimately successful in its appeal.[5][6] Subsequent reactions included the discussion of secret subpoenas in the U.S.,[7] criticism of the particular subpoena issued,[7][8][9] an immediate,[4] temporary[10] 0.5 percent reduction in the number of Twitter followers of [redacted] and calls for the recognition and emulation of Twitter's stance.[11]

Contents

Chronology

Prior to the December 2010 subpoena relating to [redacted], Twitter had received at least one subpoena for information about its users. Just after the Attorney-General of the US state of Pennsylvania Tom Corbett was elected as governor of Pennsylvania, it was revealed that he had issued a subpoena against Twitter to demand personal information on two users who criticised him.[12] *The Philadelphia Inquirer* claimed that the subpoena was issued because of the two users' criticisms of Corbett.[12] Corbett's spokesperson said that the subpoena was issued as "part of an ongoing criminal investigation".[12] The two users were helped by Public Citizen and the American Civil Liberties Union (ACLU) in opposing the subpoena.[13] The subpoena was "dropped" by the Attorney-General's office.[13]

Subpoena issued with accompanying gag order

On 14 December 2010 the U.S. Department of Justice issued a subpoena directing Twitter to hand over information in accordance with 18 USC § 2703 (d) (http://www.law.cornell.edu/uscode/uscode18/usc_sec_18_00002703----000-.html) . The order additionally directed that Twitter should not disclose the existence of the subpoena without prior authorization. Issued in relation to ongoing investigations of [redacted], named were [redacted] The requisite information included their user names, addresses, telephone numbers, bank account details, and credit card numbers.[2]

[redacted] lawyer Mark Stephens argued that[3] since the application also extended to destination email addresses and IP addresses for any communication stored for the named accounts, personal identifying information was to be collected for some six hundred and thirty-four thousand followers of [redacted] Twitter feed.[1][2][4]

[redacted] alleged it had evidence suggesting similar subpoenas had been issued to Google and Facebook,[14] and lawyer Mark Stephens said that similar information had been sought not only from Google and Facebook but

also from EBay's Skype unit.[1] [redacted] called for Google and Facebook to unseal the subpoenas if they had received them,[14] but no spokespeople were available to comment.[1]

Appeal and publication of the subpoena

Twitter applied to notify its users of the issue of the subpoena.[5][15][16] On 5 January 2011 it was notified of success in its appeal,[6] allowing the company to inform its users and to give them ten days in turn in which to appeal.[15] After Twitter informed [redacted] she released a message via the micro-blogging site that the "USA government wants to know about all my tweets and more since november 1st 2009. Do they realize I am a member of parliament in Iceland?"[9]

Aden Fine of the ACLU said that "Twitter's e-mail indicated that it had not yet turned over to the U.S. government any records that prosecutors requested."[17]

Users' opposition to the subpoena

Among those specifically named by the subpoena, [redacted] [17] all stated that they would oppose it. Lawyer Aden Fine of the ACLU participated in defending those subpoenaed.[17] [redacted] stated that she had contacted the Icelandic Minister of Justice and Human Rights and commented that the "U.S. government is trying to criminalize whistleblowing and publication of whistleblowing material."[17]

Subsequent reactions

The New York Times observed that the US government issues over fifty thousand such requests for information each year, typically accompanied by the so-called gag order,[7] linking the case to how "1986 Privacy Law is Outrun by the Web".[18] Nicholas Merrill, the first to file a constitutional challenge against the use of national security letters, describes this as "a perfect example of how the government can use its broad powers to silence

people".[7] Lawmakers in Iceland criticised the subpoena as an instance of overreach.[8][19][9] [redacted] lawyer, Mark Stephens, interpreted the subpoena as a sign that US authorities were desperate to develop a criminal case against [redacted] He stated that the subpoena was an attempt to "shake the electronic tree in the hope some kind of criminal charge drops out the bottom of it."[14]

Juan Cole, a historian of the modern Middle East and South Asia, described the subpoena as "a fishing expedition and legally fishy in that regard" that "is being pursued by the Obama administration out of terror that further massive leaks will be made public."[20] He contrasted the legal action against people associated with [redacted] with the lack of legal actions against "Bush administration officials, such as Dick Cheney, who ordered people tortured [and] have not been in any way inconvenienced by Mssrs. Obama and Holder."[20] Cole suggested that users of social media should shift from Facebook and Twitter that have "internet monopolies" and "are in turn tools of US government control" to social media based in Europe or the Global South.

[redacted] list of 637,000 followers on Twitter dropped by 3,000 in the hours following the announcement of the US Department of Justice action[4] and grew to 650,000 as of 13 January 2011.[10]

Professor of Law Ben Saul argued that the US had been compelled to attempt to obtain information on citizens of other countries through action against its own companies due to its lack of overseas law enforcement powers, suggesting that "the real question is how will other countries react ... will other governments try to do things to shut down this kind of investigation?"[21] Members of the European Parliament from the Netherlands, Romania and the UK have questioned whether US 'snooping' on the Twitter accounts of those linked with WikiLeaks is in violation of European privacy laws.[22][23]

The Electronic Frontier Foundation has since, comparing their law enforcement policies, stressed "how important it is that social media companies do what they can to protect the sensitive data they hold from the prying eyes of the government".[24] *Wired* staff writer Ryan Singel said that Twitter's "action in asking for the gag order to be overturned sets a new

precedent that we can only hope that other companies begin to follow" and summarised his point of view by saying "Twitter beta-tested a spine" and that Twitter's response should become an "industry standard".[11]

See also

- Foreign Intelligence Surveillance Act - US Act of 1978, preventing spying on US citizens without a court order
- Electronic Communications Privacy Act - US Act of 1986, before widespread email and cellphone usage
- PATRIOT Act - US Act of 2001, introducing counter-terrorism measures
- American Civil Liberties Union v. Ashcroft (2004) - first constitutional challenge of US PATRIOT Act national security letter provisions
- Information sensitivity

References

1. ^ *a b c d e* Larson, Erik (10 January 2011). "US Twitter Subpoena on WikiLeaks is Harassment, Lawyer Says" (http://www.bloomberg.com/news/2011-01-10/u-s-twitter-subpoena-on-[redacted]-is-harassment-lawyer-says.html) . *Bloomberg*. http://www.bloomberg.com/news/2011-01-10/u-s-twitter-subpoena-on-wikileaks-is-harassment-lawyer-says.html. Retrieved 10 January 2011.
2. ^ *a b c d* "Twitter Subpoena" (http://www.webcitation.org/5vfUQlMUS) (PDF). *Salon*. Archived from the original (http://www.salon.com/news/opinion/glenn_greenwald/2011/01/07/twitter/subpoe on 11 January 2011. http://www.webcitation.org/5vfUQlMUS. Retrieved 10 January 2011.
3. ^ *a b* Whittaker, Zack (8 January 2011). "US Subpoenas Wikileaks Tweets, and Why This Could Affect You" (http://www.webcitation.org/5vfkLf0Ru) . ZDNet. Archived from the original (http://www.zdnet.com/blog/igeneration/us-subpoenas-[redacted]-tweets-and-why-this-could-affect-you/7610) on 11 January 2011. http://www.webcitation.org/5vfkLf0Ru. Retrieved 12 January 2011.
4. ^ *a b c d e* Staff writer (10 January 2011). "US Turns to Twitter as WikiLeaks Chase Continues" (http://www.webcitation.org/5vfhryW49) . *The Sydney Morning Herald*. Archived from the original (http://www.smh.com.au/technology/technology-news/us-turns-to-twitter-as-wikileaks-chase-continues-20110109-19jy5.html) on 11 January 2011. http://www.webcitation.org/5vfhryW49. Retrieved 11 January 2011.

5. ^ [a] [b] Sonne, Paul (10 January 2011). "U.S. Asks Twitter for [redacted] Data" (http://online.wsj.com/article/SB10001424052748704482704576072081788 *The Wall Street Journal*. http://online.wsj.com/article/SB10001424052748704482704576072081788251567 Retrieved 10 January 2011.
6. ^ [a] [b] "Twitter Unsealing Order" (http://www.webcitation.org/5vfUjT39u) (PDF). [redacted]. Archived from the original (http://rop.gonggri.jp/wp-content/uploads/2011/01/Twitter_Unsealing_Order.pdf) on 11 January 2011. http://www.webcitation.org/5vfUjT39u. Retrieved 11 January 2011.
7. ^ [a] [b] [c] [d] **(registration required)** Cohen, Noam (9 January 2011). "Twitter Shines a Spotlight on Secret F.B.I. Subpoenas" (http://www.nytimes.com/2011/01/10/business/media/10link.html?partner=rss&emc=rss) . *The New York Times*. http://www.nytimes.com/2011/01/10/business/media/10link.html?partner=rss&emc=rss. Retrieved 10 January 2011.
8. ^ [a] [b] Connor, Richard (9 January 2011). "Iceland Blasts US Demand for Lawmaker's Details in [redacted] Probe" (http://www.dw-world.de/dw/article/0,,14758284,00.html) . *Deutsche Welle*. http://www.dw-world.de/dw/article/0,,14758284,00.html. Retrieved 10 January 2011.
9. ^ [a] [b] [c] Rushe, Dominic (8 January 2011). "Icelandic MP Fights US Demand for Her Twitter Account Details — [redacted] Brands Efforts by US Justice Department To Access Her Private Information 'Completely Unacceptable'" (http://www.guardian.co.uk/media/2011/jan/08/us-twitter-hand-icelandic-wikileaks-messages) . *The Guardian*. http://www.guardian.co.uk/media/2011/jan/08/us-twitter-hand-icelandic-wikileaks-messages. Retrieved 10 January 2011.
10. ^ [a] [b] "Get short, timely messages from [redacted]" (http://www.webcitation.org/5viLYFKUX) . Twitter. 13 January 2011. Archived from the original (http://twitter.com/wikileaks) on 13 January 2011. http://www.webcitation.org/5viLYFKUX. Retrieved 13 January 2011.
11. ^ [a] [b] Singel, Ryan (10 January 2011). "Twitter's Response to [redacted] Subpoena Should Be the Industry Standard" (http://www.webcitation.org/5vfhxlrys) . *Wired*. Archived from the original (http://www.wired.com/threatlevel/2011/01/twitter/) on 11 January 2011. http://www.webcitation.org/5vfhxlrys. Retrieved 11 January 2011.
12. ^ [a] [b] [c] Staff writer (20 May 2010). "Corbett Subpoenas Twitter for Critics' Names" (http://www.webcitation.org/5vfac4IAo) . *The Philadelphia Inquirer*. Archived from the original (http://www.philly.com/philly/blogs/our-money/Corbett_subpoenas_Twitter_for_critics_names.html) on 11 January 2011. http://www.webcitation.org/5vfac4IAo. Retrieved 12 January 2011.

13. ^ [a] [b] Kravets, David (21 May 2010). "Pennsylvania AG Dropping Twitter Subpoena" (http://www.webcitation.org/5vfaJKgBE) . *Wired*. Archived from the original (http://www.wired.com/threatlevel/2010/05/twitter-subpoena-2/) on 11 January 2011. http://www.webcitation.org/5vfaJKgBE. Retrieved 12 January 2011.
14. ^ [a] [b] [c] Yost, Pete; Satter, Raphael G. (8 January 2011). "[redacted] Subpoenas Spill Out into Public Realm" (http://www.webcitation.org/5vfW25lha) . *Associated Press* (via *Toronto Star*). Archived from the original (http://www.thestar.com/news/world/article/918606--[redacted]-subpoenas-spill-out-into-public-realm) on 11 January 2011. http://www.webcitation.org/5vfW25lha. Retrieved 12 January 2011.
15. ^ [a] [b] Greenwald, Glenn. "DOJ Subpoenas Twitter Records of Several [redacted] Volunteers" (http://www.webcitation.org/5vfVUxx8j) . *Salon*. Archived from the original (http://www.salon.com/news/opinion/glenn_greenwald/2011/01/07/twitter) on 11 January 2011. http://www.webcitation.org/5vfVUxx8j. Retrieved 10 January 2011.
16. ^ Beaumont, Peter (8 January 2011). [redacted] Demands Google and Facebook Unseal US Subpoenas" (http://www.guardian.co.uk/media/2011/jan/08/us-twitter-hand-icelandic-wikileaks-messages) . *The Guardian*. http://www.guardian.co.uk/media/2011/jan/08/us-twitter-hand-icelandic-[redacted]-messages. Retrieved 10 January 2011.
17. ^ [a] [b] [c] [d] Hosenball, Mark (11 January 2011). "[redacted] Activists May Seek To Quash Demand for Docs" (http://www.webcitation.org/5vfiyscBG) . *Reuters*. Archived from the original (http://www.reuters.com/article/idUSTRE70A5ZT20110111) on 11 January 2011. http://www.webcitation.org/5vfiyscBG. Retrieved 12 January 2011.
18. ^ "1986 Privacy Law is Outrun by the Web" (http://www.nytimes.com/2011/01/10/technology/10privacy.html?partner=rss&emc=rss) . *The New York Times*. http://www.nytimes.com/2011/01/10/technology/10privacy.html?partner=rss&emc=rss. Retrieved 13 January 2011.
19. ^ Menn, Joseph *et al.* (8 January 2011). "Iceland Protests over US Probe of Lawmaker" (http://www.ft.com/cms/s/0/7edd3e2a-1b52-11e0-868c-00144feab49a.html#axzz1AdqdyPId) . *The Financial Times*. http://www.ft.com/cms/s/0/7edd3e2a-1b52-11e0-868c-00144feab49a.html#axzz1AdqdyPId. Retrieved 10 January 2011.
20. ^ [a] [b] Cole, Juan (8 January 2011). "DOJ Subpoenas Twitter Account of [redacted] Volunteer and Now [redacted] MP" (http://www.webcitation.org/5vfcfKKYI) . Juan Cole. Archived from the original (http://www.juancole.com/2011/01/doj-subpoenas-twitter-account-of-[redacted]-volunteer-and-now-iceland-mp.html) on

11 January 2011. http://www.webcitation.org/5vfcfKKYI. Retrieved 12 January 2011.

21. ^ Sherington, Greg (11 January 2011). "US Subpoena of Iceland Twitter Accounts" (http://sydney.edu.au/news/law/436.html?newscategoryid=67&newsstoryid=6261) . Sydney Law School. http://sydney.edu.au/news/law/436.html?newscategoryid=67&newsstoryid=6261. Retrieved 13 January 2011.
22. ^ "Anonymous urges global protests" (http://www.bbc.co.uk/news/technology-12191486) . BBC. http://www.bbc.co.uk/news/technology-12191486. Retrieved 17 January 2011.
23. ^ "ALDE Calls on Commission to clarify issue of US Government [redacted]) subpoenas" (http://www.alde.eu/press/press-and-release-news/press-release/article/alde-calls-on-commission-to-clarify-issue-of-us-government-wikileaks-subpoenas-36732/) . Alliance of Liberals and Democrats for Europe. http://www.alde.eu/press/press-and-release-news/press-release/article/alde-calls-on-commission-to-clarify-issue-of-us-government-[redacted]-subpoenas-36732/. Retrieved 17 January 2011.
24. ^ "Social Media and Law Enforcement: Who Gets What Data and When?" (http://www.eff.org/deeplinks/2011/01/social-media-and-law-enforcement-who-gets-what) . Electronic Frontier Foundation. http://www.eff.org/deeplinks/2011/01/social-media-and-law-enforcement-who-gets-what. Retrieved 22 January 2011.

External links

- Twitter Help Center: Guidelines for Law Enforcement (http://support.twitter.com/entries/41949-guidelines-for-law-enforcement)

Retrieved from "http://en.wikipedia.org/wiki/Twitter_subpoena"
Categories: Privacy of telecommunications | Twitter | WikiLeaks

GOVERNMENT EXHIBIT 6

[redacted]

From: [redacted]@gmail.com]
Sent: Wednesday, January 12, 2011 4:25 AM
To: [redacted]

You guys are fucking nazis trying to controll the whole fucking world.
Well guess what.

WE DO NOT FORGIVE.
WE DO NOT FORGET.
EXPECT US.

FILED

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

2011 JAN 18 P 12:58

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

IN RE 2703(d) ORDER AND 2703(f) PRESERVATION REQUEST RELATING TO GMAIL ACCOUNT [redacted]	Misc. No. 10GJ3793 FILED UNDER SEAL

NOTICE OF HEARING

PLEASE TAKE NOTICE that, by agreement with the United States Attorney's Office and subject to consultation with chambers, on February 2, 2011 at 9:00 a.m., or as soon thereafter as possible, Google Inc. will bring on for hearing its Motion to Modify 2703(d) Order for Purpose of Providing Notice to User. This motion will be heard in the Albert V. Bryan United States Courthouse, 401 Courthouse Square, Alexandria, VA 22314.

DATED this 18th day of January, 2011.

Respectfully submitted,

By _____

John K. Roche (VSB# 68594)
~~Perkins Coie~~ LLP
700 13th St., N.W., Suite 600
Washington, D.C. 20005-3960
Phone: 202-434-1627
Fax: 202-654-9106
JRoche@perkinscoie.com

Albert Gidari (*pro hac vice pending*)
Perkins Coie LLP
1201 Third Avenue, Suite 4800
Seattle, Washington 98101
Phone: 206.359.8000
Fax: 206.359.9000
AGidari@perkinscoie.com

Attorneys for Google Inc.

CERTIFICATE OF SERVICE

I hereby certify that on this 18th day of January, 2011, the foregoing document was sent via hand delivery and email to the following persons:

[redacted]
Assistant United States Attorney
United States Attorney's Office
Eastern District of Virginia
Justin W. Williams United States Attorney's Building
2100 Jamieson Avenue
Alexandria, VA 22314-5794
[redacted] facsimile)

Attorneys for the United States

By _____
John K. Roche (VSB# 68594)
Perkins Coie, LLP
700 13th St., N.W., Suite 600
Washington, D.C. 20005-3960
Phone: 202-434-1627
Fax: 202-654-9106
JRoche@perkinscoie.com

Attorneys for Google Inc.

ATTACHMENT C

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

FILED

2011 FEB -1 P 3:35

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

IN RE 2703(d) ORDER AND 2703(f) PRESERVATION REQUEST RELATING TO GMAIL ACCOUNT [redacted]	Misc. No. 10GJ3793 FILED UNDER SEAL

GOOGLE INC.'S REPLY IN SUPPORT OF ITS MOTION TO MODIFY 2703(d) ORDER FOR PURPOSE OF PROVIDING NOTICE TO ACCOUNT HOLDER

Google Inc. ("Google") hereby submits this Reply in Support of its Motion to Modify 2703(d) Order for Purpose of Providing Notice to Account Holder.

The government admits in its response brief that the demand at issue here (the "Order")[1] and the unsealed Twitter Order[2] relate to the same investigation. The government's brief also establishes that the targets of their investigation are already operating under the assumption that the government has sought information related to their Google accounts. These facts alone demonstrate that there is no cause for the Order to have been sealed in the first place or to remain sealed now. Moreover, rather than demonstrating how unsealing the Order will harm its well-publicized investigation, the government lists a parade of horribles that have allegedly occurred since it unsealed the Twitter Order, yet fails to establish how any of these developments could be further exacerbated by unsealing this Order. The proverbial toothpaste is out of the tube, and continuing to seal a materially identical order will not change it.

[1] *See* Declaration of John K. Roche, Ex. 1 ("Roche Decl.").

[2] *Id.* Ex. 2.

The government also prejudges any free speech or privilege objections that Google's user may wish to raise by describing them as "meritless." Of course, if the user's potential arguments are all so obviously meritless as to not even warrant a hearing, one is left to wonder why the government agreed to unseal the Twitter Order in the first place in order to allow those users an opportunity to file their objections. Indeed, the Twitter use[redacted]may have already filed an opposition to the Twitter Order with this Court. If he or she has, it would certainly be incongruous for this Court to hear those objections in relation to the Twitter Order, but to foreclose any opportunity to hear objections in relation to this Order based solely on the government's generalized ex parte and wholly speculative assertion that those objections are frivolous. We specifically ask that the government advise the Court whether such objections have been filed or motions made in regard to the Twitter order.

Accordingly, for these reasons and those stated below and in Google's motion, Google respectfully requests that the Court grant its motion and modify the Order pursuant to the terms of Google's proposed order.

I. ARGUMENT

A. The Government's Response Confirms There is No Need for Secrecy of this Order or the Preservation Request

The government admits that the Twitter Order and the Order involve the same investigation, yet inscrutably claims that the Order must remain sealed because it involves "a different case" than the Twitter Order. *See* Government Response, at 3 n.1; *see also id.* at 13. This opaque rationale for refusing to unseal the Order does not withstand scrutiny.

As noted in Google's motion, the Order does not meet any of the traditional standards for

grand jury confidentiality. *See* Google's Motion, at 9. Specifically, the Wikileaks investigation and the government's interest in [redacted] electronic communications are already a well-publicized matter of public record. *McHan v. C.I.R.*, 558 F.3d 326, 334 (4th Cir. 2009) ("it is a 'common-sense proposition that secrecy is no longer "necessary" when the contents of grand jury matters have become public.'") (quoting *In re Grand Jury Subpoena,* 438 F.3d 1138, 1140 (D.C. Cir. 2006)).

Furthermore, disclosure of the Order would not reveal any witness testimony, so there is no fear of retribution against witnesses as a result. *Finn v. Schiller*, 72 F.3d 1182, 1187 n.6 (4th Cir. 1996). The government claims that unsealing the Order may result in "witness intimidation" in the form of encouraging providers "to resist the government's attempts to gather relevant user information." *See* Government Response, at 16. This argument is specious. First, keeping orders in the shadows to prevent witness intimidation is one thing, but doing so to prevent public discourse is not a proper use of the mechanism. Second, providers are corporate entities advised by competent inside and outside counsel, some of whom are former government attorneys. The notion that these companies could be intimidated into resisting otherwise valid legal process is baseless. Google can only speak for itself, but when it resists legal process, it does so because its attorneys have a good faith belief that the process is deficient or unlawful in some respect, not because Google is trying to curry favor with some interest group. Google has no reason to believe that other providers' approach to legal process is any different.

Additionally, there is no risk of destruction of evidence because Google has preserved responsive information and the Order only demands historical records, not prospective data. The government nevertheless argues that unsealing this Order may cause the targets to "alter[] their modes of communication to evade future investigative efforts," but as the government notes in

its brief, the Twitter user [redacted]nd other targets of the investigation are already working under the assumption that their Google accounts are the subject of legal process from this grand jury investigation. *See* Government Response, at 14; *see also* Government Exhibits 3-4. Therefore, disclosing this Order will do nothing to alter anyone's behavior, and to the extent ioerror has already destroyed evidence, unsealing the Order will not reverse those actions either.

The government also claims that the Order must remain sealed "because it might cause suspects to . . . flee." *See* Government Response, at 13. This argument also fails because if [redacted] is a flight risk, the widespread media coverage of the Twitter Order would have already presumably given him or her and any co-conspirators all the notice they need to start packing their bags, regardless of whether Twitter's [redacted] and Google's [redacted] are one and the same.

Finally, the government asserts that its employees were harassed after the disclosure of the Twitter Order and implies that the same can be expected if this Order is disclosed. *See* Government Response, at 15-16; *see also* Government Exhibit 6. Google condemns any such attacks on government personnel and sympathizes with those forced to endure them. In order to ensure that the same behavior does not occur here, the government should request that the court order any personal identifiers of government personnel redacted before unsealing the Order or preservation letter.

In sum, there is no risk of destruction evidence, and none of the other interests served by the traditional secrecy of grand jury proceedings would be undermined in any way by disclosure of the Order or the preservation request. There is no cause for the Order to remain sealed.

B. The Court Should Grant [redacted] the Opportunity to Assess the Legality of the Order

Google understands that Twitter's [redacted]ser and the other users affected by the Twitter Order were granted a certain period of time in which to file their opposition to the Twitter Order. *See* Government Exhibit 5. The government should disclose whether or not such filings have been made. If Twitter's [redacted]ser did indeed file an opposition brief, it would be logical to assume there is an excellent chance that Google's [redacted] would similarly oppose this Order if one assumes the user is the same. Worse, the user and the Court hearing any such motions are misled into believing that only the Twitter Order is at issue when considering the scope of harm to the user and any First Amendment or other rights that are implicated by the government's demands.[3]

Google therefore suggests that the Court ask the government at oral argument whether the user for the [redacted] Twitter account has filed an opposition with this Court to the Twitter Order. If the user has, Google respectfully submits that the Court should not collaterally prejudge the merits of that opposition by accepting the government's assertions that any arguments raised by Google [redacted] in response to the Order "would be meritless." *See* Government Response, at 6. I[redacted]s arguments are meritless, then the government has nothing to fear. On the other hand, if [redacted]s arguments are valid, the user should be permitted to raise them here, just as Twitter's [redacted] user may have already done in regard to the Twitter Order. Regardless, not informing Google's [redacted]f the Order at the same time Twitter's [redacted] may be asserting his or her rights in regard to the materially identical Twitter Order seems unfair to the user.

[3] Indeed, Google is not privy to all the orders that may have been issued to all the providers of services to user [redacted] but the Court hearing any motion to quash or amend the Twitter Order, or to unseal a pending order such as here, ought to be made aware of the scope of such inquiry.

Furthermore, Google made clear in its motion that it is not in the best position to advocate for the free speech or other privilege rights of its users – the users are. Nevertheless, the government has seen fit to denigrate any potential arguments that Google's user might raise, even though those potential arguments are not as easily disposed of as the government suggests. For example, the government is dismissive of the fact that Wikileaks has been widely described as an enterprise that consists of, or works with, journalists and academics.[4] While Google does not comment on whether this is an accurate description of what Wikileaks does, one can assume that if [redacted] is somehow associated with Wikileaks, he or she may wish to assert his or her own First Amendment rights or any applicable journalistic, academic or other privileges or defenses to which [redacted] feels he or she is entitled. [redacted] might assert that the Order's demand for "the source and destination email addresses and IP addresses" for communications in his or her account will reveal confidential sources or information about Wikileaks' purported journalistic or academic activities. The extent to which such sources and information are protected from discovery by the grand jury is a hotly debated issue, and one that [redacted] may wish to raise before this Court. *In re Grand Jury Subpoena, Judith Miller*, 438 F.3d 1141, 1164 (D.C. Cir. 2006) (Tatel, J., concurring) (the Supreme Court's *Branzburg* decision "places limits on grand jury authority to demand information about source identities – though, again, the precise extent of those limits seems unclear."); *id.* at 1174 ("Of course, in some cases a leak's value may far

[4] *See, e.g., Salmeron v. Enterprise Recovery Systems, Inc.*, 579 F.3d 787, 791 n.1 (7th Cir. 2009) ("'[F]ounded by Chinese dissidents, journalists, mathematicians and startup company technologists, from the US, Taiwan, Europe, Australia and South Africa,' Wikileaks styles itself as 'an uncensorable version of Wikipedia for untraceable mass document leaking and analysis.' http:// wikileaks. org/ wiki/ Wikileaks: About (last visited July 16, 2009)."); Adam L. Penenberg, *Yes, He's a Journalist, Too,* Washington Post, Jan. 30, 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/01/28/AR2011012806860.html ("Based on the wording of many of these [press shield] statutes, Assange fits the definition of a journalist, and what WikiLeaks does qualifies as journalism.") (last visited on Jan. 30, 2011); *US soldiers can be demoralized by WikiLeaks docs: Morrell*, Daily Pak Banker, Oct. 25, 2010, 2010 WLNR 21356017 (describing Wikileaks as working with "a group run by academics"); *Activists targeted as secrets exposed*, Australian, Apr. 12, 2010, 2010 WLNR 7507448 (describing Wikileaks as consisting of "computer programmers, academics and activists.").

exceed its harm, thus calling into question the law enforcement rationale for disrupting reporter-source relationships."); *In re Grand Jury Subpoena Dated Jan. 4, 1984*, 750 F.2d 223, 225 (2d Cir. 1984) ("Surely the application of a scholar's privilege, if it exists, requires a threshold showing consisting of a detailed description of the nature and seriousness of the scholarly study in question, of the methodology employed, of the need for assurances of confidentiality to various sources to conduct the study, and of the fact that the disclosure requested by the subpoena will seriously impinge upon that confidentiality."); *U.S. v. Doe*, 460 F.2d 328, 334 (1st Cir. 1972) (grand jury questions "seeking the names of persons interviewed who gave [a university professor] knowledge of participants in the Pentagon Papers study should be answered, *at least to the extent that the persons were not government officials or other participant-sources*.") (emphasis added).

Conversely, [redacted] may simply be an independent party who has voiced support for Wikileaks. If so, that activity is at the core of free speech and is certainly entitled to protection. *Gentile v. State Bar of Nevada*, 501 U.S. 1030, 1034 (1991) ("There is no question that speech critical of the exercise of the State's power lies at the very center of the First Amendment.").

In any event, the point is that [redacted] – not Google or the government – is in the best position to assess the propriety of any legal process related to the [redacted] Gmail account, and the Court should have the opportunity to hear the objections. *In re Grand Jury Subpoena*, 438 F.3d at 1164 (Tatel, J., concurring) ("given that any witness – journalist or otherwise – may challenge [an unreasonable or oppressive] subpoena, the majority [in *Branzburg*] must have meant, at the very least, that the First Amendment demands a broader notion of 'harassment' for journalists than for other witnesses.").

C. The Order is a Prior Restraint on Google's Right to Free Speech

Finally, while arguments raised for the first time in reply are generally not considered, Google must correct the government's erroneous assertion that "Google has no viable First Amendment argument to make on its own behalf." *See* Government Response, at 6. On the contrary, the non-disclosure provision in the Order certainly prevents Google from communicating with its user and "is fairly characterized as a regulation of pure speech." *Bartnicki v. Vopper*, 532 U.S. 514, 526 (2001) (referring to Wiretap Act provision prohibiting disclosure of contents of illegally intercepted communication). The Order's non-disclosure provision also prevents Google from defending itself against public criticism such as that cited in the Government's brief. *See* Government Exhibits 3-4. It is of no moment that the person it restrains from speaking, *i.e.*, Google, is a corporate entity. *First Nat'l Bank of Boston v. Bellotti*, 435 U.S. 765, 777 (1978) ("The inherent worth of the speech in terms of its capacity for informing the public does not depend upon the identity of its source, whether corporation, association, union, or individual."). Prior restraints on speech "are constitutionally disfavored in this nation nearly to the point of extinction." *United States v. Brown*, 250 F.3d 907, 915 (5th Cir. 2001). Accordingly, such restraints are subject to the most demanding scrutiny. *In re Sealing and Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 881-82 (S.D. Tex. 2008) ("Prohibiting a service provider from disclosing the existence of the pen/trap or the investigation means that the first-hand experiences of the recipients of these orders are completely excluded from the public debate" and "dries up the marketplace of ideas just as effectively as a customer-targeted injunction would do."). While Google certainly could have made its own First Amendment arguments, and this Court certainly may consider them on its own, the point of Google's motion was to ensure that its user had the opportunity to assert such rights.

Here, the government has offered to limit the nondisclosure requirement in the Order to a period of 90 days, with a provision allowing it to petition the Court for extensions if disclosure would seriously jeopardize the investigation or have an adverse result as defined by 18 U.S.C. § 2705(a)(2). Google agrees that such nondisclosure requirements of a limited duration are not uncommon in normal investigations, and are rarely challenged by providers. However, this is not a normal investigation. Because the government's interest in [redacted] electronic communications is already so well-publicized and there is absolutely no risk of destruction of evidence, Google fails to see how any nondisclosure period is justified under these highly unique and unusual circumstances.

II. CONCLUSION

For the reasons stated here and in Google's motion, Google respectfully requests that the Court grant its motion and modify the Order pursuant to the terms of Google's proposed order.

DATED this 1st day of February, 2011.

Respectfully submitted,

By _____

John K. Roche (VSB# 68594)
Perkins Coie LLP
700 13th St., N.W., Suite 600
Washington, D.C. 20005-3960
Phone: 202-434-1627
Fax: 202-654-9106
JRoche@perkinscoie.com

Albert Gidari (*pro hac vice pending*)
Perkins Coie LLP
1201 Third Avenue, Suite 4800
Seattle, Washington 98101
Phone: 206.359.8000
Fax: 206.359.9000
AGidari@perkinscoie.com

Attorneys for Google Inc.

CERTIFICATE OF SERVICE

I hereby certify that on this 1st day of February, 2011, the foregoing document was sent via hand delivery and email to the following persons:

[redacted]
Assistant United States Attorney
United States Attorney's Office
Eastern District of Virginia
Justin W. Williams United States Attorney's Building
2100 Jamieson Avenue
Alexandria, VA 22314-5794
703-[redacted]
703-

Attorneys for the United States

By _____
John K. Roche (VSB# 68594)
Perkins Coie, LLP
700 13th St., N.W., Suite 600
Washington, D.C. 20005-3960
Phone: 202-434-1627
Fax: 202-654-9106
JRoche@perkinscoie.com

Attorneys for Google Inc.

ATTACHMENT D

THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE 2703(d) ORDER AND 2703(f) PRESERVATION REQUEST RELATING TO GMAIL ACCOUNT	Case No. 1:10GJ3793 11-DM-2 **UNDER SEAL**

MOTION TO CONTINUE HEARING

The United States by and through [redacted] United States Attorney, and [redacted] Assistant United States Attorney, hereby moves this Court to continue the hearing scheduled Friday, February 4, 2011, on Google's Motion to Modify the Court's § 2703(d) Order to authorize Google to provide notice of the Order to its account holder. Google Inc.'s ("Google") reply to the government's response raises a concern that a decision by this Court would "prejudge[] any free speech or privilege objections that Google's user may wish to raise by describing them as meritless." Google Reply at 2, 5-7. As counsel for Google knows,[1] the account holder in this case has already filed a motion, objecting to a similar § 2703(d) Order issued by Magistrate Judge [redacted] Therefore, Google's concerns with speculating about the user's objections are best addressed by awaiting a decision on their merits.

[1] In its reply, Google asked "that the government advise the Court whether such objections have been filed or motions made in regard to the Twitter order." Google Reply at 2, 5. Although the motions are under seal, because counsel represents both Twitter and Google in these separate matters, counsel is well aware that further motions have been made with respect to the Twitter Order. This is so because Twitter's compliance with the Twitter Order with respect to certain user accounts is stayed pending resolution of objections filed by those users.

On December 14, 2010, Magistrate Judge [redacted] issued an order under 18 U.S.C. § 2703(d) ("the Twitter Order") requiring the online micropublishing company Twitter to provide the government with information about certain of its users, including one using the name [redacted] Counsel for Google, John Roche, who also serves as counsel for Twitter, knows this because the Twitter Order was unsealed on January 5, 2011 and both the unsealing order and the Twitter Order were publicly posted on the Internet as part of an online article, whose author presumably received them from one of Twitter's account holders.

Meantime, on January 4, 2011, this Court issued a § 2703(d) order ("the Google Order") requiring Google to provide the government with information about one of its users, named [redacted]" Since then, Google has largely adopted Twitter's legal strategy, both by filing its own motion to provide its user with the opportunity to contest the Google Order, and, within its filings, identifying itself with Twitter and its arguments. In its Motion, Google described the Google Order and the Twitter Order as "nearly identical," Google Mot. at 1, and argued that the Google Order "like the Twitter Order" raised First Amendment concerns, Google Mot. at 2. Google continues this tack in its Reply brief, arguing that it would be "incongruous" for the Court to hear arguments from Twitter users, but not from Google users, and asking the government to advise it whether Twitter users have lodged objections, presumably so Google users may assert those objections here. Google Reply at 2, 5.

To a considerable extent Google has argued that, as Twitter goes, so goes Google. *See* Google Reply at 5-7. In the event Magistrate Judge [redacted] rules in favor of the relevant Twitter account holder, Google's motion to disclose the Google Order to its account holder would be all the more compelling. The opposite also holds true. Therefore, the United States respectfully requests that this Court continue the hearing on Google's instant motion until Judge

[redacted] has ruled on the merits of the objections raised by the relevant Twitter account holder. The government expects resolution of this within the next few weeks, and therefore, the continuance would be brief.

The United States has contacted counsel for Google, who opposes this motion to continue. Nevertheless, for the reasons stated above, pursuant to Local Criminal Rule 47, good cause supports the requested brief continuance, which will not prejudice Google or the relevant account user. Therefore the United States requests this Court to continue the hearing scheduled Friday, February 4, 2011.

Respectfully Submitted,

[redacted]
United States Attorney

By: [redacted]
Assistant United States Attorney

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing pleading was delivered on this 3rd day of February 2011 to the Clerk's Office and that service will be made on the following individuals by electronic mail and otherwise:

John K. Roche, Esquire
Perkins Coie LLP
700 13th St., N.W., Suite 600
Washington, D.C. 20005-3960
PHONE: 202.434.1627
FAX: 202.654.9106
E-MAIL: JRoche@perkinscoie.com

[redacted]
Assistant United States Attorney

THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE 2703(d) ORDER AND 2703(f) PRESERVATION REQUEST RELATING TO GMAIL ACCOUNT	Case No. 1:10GJ3793 11-DM-2 **UNDER SEAL**

ORDER

This matter having come before the Court pursuant to the motion of the United States to continue the hearing on the above-captioned matter from February 4, 2011 until February 25, 2011, and finding pursuant to Local Criminal Rule 47 that good cause supports the requested continuance, it is hereby ORDERED that the hearing is postponed until February 25, 2011.

[redacted]
United States Magistrate Judge

Date: _____

Alexandria, Virginia

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing proposed order was delivered on this 3rd day of February 2011 to the Clerk's Office and that service will be made on the following individuals by electronic mail and otherwise:

John K. Roche, Esquire
Perkins Coie LLP
700 13th St., N.W., Suite 600
Washington, D.C. 20005-3960
PHONE: 202.434.1627
FAX: 202.654.9106
E-MAIL: JRoche@perkinscoie.com

[redacted]
Assistant United States Attorney

ATTACHMENT E

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

IN RE 2703(d) ORDER AND 2703(f) PRESERVATION REQUEST RELATING TO GMAIL ACCOUT [redacted]	)	Misc. No. 10GJ3793 FILED UNDER SEAL

ORDER

FOR REASONS stated from the bench and in accord with specific rulings and instructions thereto, it is hereby

ORDERED that Google's Motion to Modify 2703(d) Order for Purpose of Providing Notice to User is **DENIED in part and GRANTED in part**; the motion is **DENIED** as to Google's request to notify the user concerning the 2703(d) Order and the underlying application; the motion is **GRANTED** in regard to the request to modify the Order. In that regard, it is further

ORDERED that Google is authorized to provide notification of this Court's 2703(d) Order, dated January 4, 2011, to the Google Gmail user [redacted] within (90) days of providing to the United States government the information requested in said Order, unless the government files a motion for an extension of that non-notification period; it is further

ORDERED that the government may request an extension of the non-notification period for a maximum of sixty (60) days.

A TRUE COPY, TESTE:
CLERK, U.S. DISTRICT COURT

BY [redacted]
DEPUTY CLERK

The Clerk is directed to file this Order under Seal and to forward copies of this Order to all counsel of record.

ENTERED this 9th day of February 2011.

[redacted]
United States Magistrate Judge

Alexandria, Virginia

ATTACHMENT F

FILED

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

2011 FEB 17 P 3:38

CLERK U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA

IN RE 2703(d) ORDER AND 2703(f) PRESERVATION REQUEST RELATING TO GMAIL ACCOUNT [redacted]	Misc. No. 1:11DM3 11-DM-2 FILED UNDER SEAL

GOOGLE INC.'S OBJECTIONS TO MAGISTRATE'S ORDER OF FEBRUARY 9, 2011 AND NOTICE OF APPEAL PURSUANT TO FED. R. CRIM. P. 59 AND MEMORANDUM IN SUPPORT

I. INTRODUCTION

This matter involves a grand jury investigation of the Wikileaks publication of State Department cables and related matters. The fact of the investigation has been widely reported in the *New York Times* and other news publications, across the Internet and around the globe.[1] Demands have been made to third party service providers, including Google Inc. ("Google"), seeking compelled disclosure of information such as with whom the subject users of those services communicated and which computers they used to do so. The Google Gmail user [redacted] is the subject of the demand at issue here (the "Order").[2] Because of the already public nature of the Wikileaks investigation, and the fact that a nearly identical order to Twitter involving the same account identifier [redacted] had been unsealed by this Court in the same

[1] *See, e.g.*, Scott Shane and John F. Burns, *U.S. Subpoenas Twitter Over WikiLeaks Supporters*, N.Y. Times, Jan. 8, 2011, http://www.nytimes.com/2011/01/09/world/09wiki.html (last visited Jan. 13, 2011); Anthony Boadle, *U.S. orders Twitter to hand over Wikileaks records*, Reuters, Jan. 8, 2011, http://www.reuters.com/article/idUSTRE70716420110108 (last visited Jan. 14, 2011); Ravi Somaiya, *Release on Bail of WikiLeaks Founder Is Delayed by Appeal*, N.Y. Times, Dec. 14, 2010, *available at* http://www.nytimes.com/2010/12/15/world/europe/15assange.html?src=twrhp (last visited Jan. 3, 2011); *Assange attorney: Secret grand jury meeting in Virginia on WikiLeaks*, CNN Justice, Dec. 13, 2010, http://articles.cnn.com/2010-12-13/justice/wikileaks.investigation_1_julian-assange-wikileaks-case-grand-jury?_s=PM:CRIME (last visited Jan. 3, 2011); Dan Goodin, *Grand jury meets to decide fate of WikiLeaks founder*, The Register, Dec. 13, 2010, *available at* http://www.theregister.co.uk/2010/12/13/assange_grand_jury/ (last visited Jan. 3, 2011).

[2] *See* Declaration of John K. Roche, Ex. 1 ("Roche Decl.").

Grand Jury proceeding ("Twitter Order"),[3] Google filed a motion to modify the Order. Google's motion requested that it be permitted to give notice of the Order to the Gmail user and the user's attorney so they would have a meaningful opportunity to contest the request. Shortly after Google filed its motion, the user identified in the Twitter Order filed his own motion to vacate the Twitter Order.[4] That motion was unsealed by this Court and posted on the Internet by the user's attorneys on February 8, 2011.[5] Despite the publicity surrounding the Twitter Order and the related motions, on February 9, 2011, Magistrate Judge [redacted] denied Google's request to provide immediate notice of the Order to its user.[6] Instead, Magistrate Judge [redacted] authorized Google to provide notice of the Order to the user 90 days after production unless the government obtained a maximum 60-day extension of the non-notification period.[7]

Google respectfully objects to Magistrate Judge [redacted] ruling because the government's investigation of Wikileaks generally, and its interest in the [redacted] user name specifically, is a matter of public record, thus obviating the need for this Order's nondisclosure provision. Furthermore, the Order, like the Twitter Order, may present substantial constitutional and statutory issues that the user may wish to raise before this Court. Additionally, given that the Order's nondisclosure provision is a prior restraint on Google's First Amendment right to communicate with its users, a nondisclosure period of any length is not justified under these circumstances. Finally, Google has preserved the requested records, thus there is no danger of

[3] Roche Decl., Ex. 2

[4] *Id.* Ex. 3.

[5] *See* Electronic Frontier Foundation, *Legal Battle Over Government Demands for Twitter Records Unsealed by Court*, Feb. 8, 2011, http://www.eff.org/press/archives/2011/02/08 (last visited on Feb. 16, 2011).

[6] *Id.* Ex. 4.

[7] *Id.*

loss or destruction of the information sought. Accordingly, Google requests that the Court modify this Order to permit notice of the Order and preservation request to be given to Google's user and attorney and that the user be given 20 days from the date of the Court's order to seek any relief.

II. FACTUAL BACKGROUND

A. Relevant Actors

Google provides electronic mail services to the public through its Gmail service. Google assiduously protects the privacy and free speech rights of its Gmail users, as evidenced by its opposition, with the support of the U.S. State Department, to the Chinese government's attack on the Gmail accounts of Chinese human rights activists.[8]

Google's general practice and preference, when addressing legal demands such as court orders, is to give notice to the account holders, whenever it is permissible and practical to do so. Even where the government asserts that disclosure to the user may have an adverse impact on an investigation, or where an order is sealed but nonetheless raises serious Constitutional concerns, Google may move to unseal the order or seek permission to notify its users.

Google recognizes that such notice is important because its users are better situated to assert their rights under the Constitution or other applicable privileges and articulate their concerns to the Court. It is for those reasons that Google asks the Court to unseal the Order as the Court did for another provider in the same Grand Jury proceeding.

[8] Andrew Jacobs and Miguel Helft, *Google, Citing Attack, Threatens to Exit China,* N.Y. Times, Jan. 13, 2011, http://www.nytimes.com/2010/01/13/world/asia/13beijing.html?_r=1&pagewanted=print (last visited Jan. 13, 2011).

Wikileaks describes itself as a journalistic enterprise for mass document leaking and analysis,[9] and has been described by others as an enterprise that consists of, or works with, journalists and academics.[10] Whether Wikileaks does in fact consist of journalists or academics or engage in journalism is a matter of public debate, and an issue upon which Google does not comment.

Twitter is a real-time information network that has been described by one federal district court as "a social networking and micro-blogging service that invites its users to answer the question: 'What are you doing?'" *U.S. v. Shelnutt*, No. 4:09-CR-14 (CDL), 2009 WL 3681827, at *1 n.1 (M.D. Ga. Nov. 2, 2009) ("Twitter's users can send and read electronic messages known as 'tweets.' A tweet is a short text post (up to 140 characters) delivered through Internet or phone-based text systems to the author's subscribers. Users can send and receive tweets in several ways, including via the Twitter website.").

Although Google does not comment on and could not confirm whether the Twitter account [redacted] is controlled by the same user as the Gmail [redacted] account, it is instructive to

[9] *Salmeron v. Enterprise Recovery Systems, Inc.*, 579 F.3d 787, 791 n.1 (7th Cir. 2009) ("'[F]ounded by Chinese dissidents, journalists, mathematicians and startup company technologists, from the US, Taiwan, Europe, Australia and South Africa," Wikileaks styles itself as 'an uncensorable version of Wikipedia for untraceable mass document leaking and analysis.' http:// wikileaks. org/ wiki/ Wikileaks: About (last visited July 16, 2009).").

[10] Adam L. Penenberg, *Yes, He's a Journalist, Too*, Washington Post, Jan. 30, 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/01/28/AR2011012806860.html ("Based on the wording of many of these [press shield] statutes, Assange fits the definition of a journalist, and what WikiLeaks does qualifies as journalism.") (last visited on Jan. 30, 2011); *US soldiers can be demoralized by WikiLeaks docs: Morrell*, Daily Pak Banker, Oct. 25, 2010, 2010 WLNR 21356017 (describing Wikileaks as working with "a group run by academics"); *Activists targeted as secrets exposed*, Australian, Apr. 12, 2010, 2010 WLNR 7507448 (describing Wikileaks as consisting of "computer programmers, academics and activists.").

note that in a "tweet," the Twitter user [redacted] indicates that since at least mid-December 2010 [redacted] has been well aware that a government investigation is underway.[11]

B. Procedural Posture

The Twitter Order was issued on December 14, 2010 and relates to the ongoing Wikileaks investigation, which is obviously an issue of great public interest.[12] The Twitter Order demanded the production of subscriber information and certain records and other non-content information for a number of Twitter account holders from November 1, 2009 to the present, including an account with the user name [redacted] It also contained a non-disclosure provision. The grand jury investigation underlying the Twitter Order was widely reported in the *New York Times* and other media outlets around the time the Twitter Order was issued.[13] Indeed, prior to issuance of the order, the Attorney General had acknowledged that the government was actively investigating Wikileaks.[14]

---

[11] *See* [redacted]" tweet of Dec. 17, 2010 @ 4:22 p.m. ("Unrelated to any travel issues - the FBI is now actively bothering my friends and questioning them inside the United States."), http://twitter.com/[redacted]/status/15879462465835008 (last visited on Dec. 21, 2010); *see also* "[redacted] tweet of Jan. 7, 2011 @ 9:26 p.m. ("Note that we can assume Google & Facebook also have secret US government subpoenas. They make no comment. Did they fold?"), http://twitter.com/[redacted] (last visited Jan. 18, 2011).

[12] Roche Decl., Ex. 2.

[13] Ravi Somaiya, *Release on Bail of WikiLeaks Founder Is Delayed by Appeal*, N.Y. Times, Dec. 14, 2010, http://www.nytimes.com/2010/12/15/world/europe/15assange.html?src=twrhp (last visited Jan. 3, 2011); *see also Assange attorney: Secret grand jury meeting in Virginia on WikiLeaks*, CNN Justice, Dec. 13, 2010, http://articles.cnn.com/2010-12-13/justice/wikileaks.investigation_1_julian-assange-wikileaks-case-grand-jury?_s=PM:CRIME (last visited Jan. 3, 2011); Dan Goodin, *Grand jury meets to decide fate of WikiLeaks founder*, The Register, Dec. 13, 2010, http://www.theregister.co.uk/2010/12/13/assange_grand_jury/ (last visited Jan. 3, 2011).

[14] Ellen Nakashima & Jerry Markon, *WikiLeaks founder could be charged under Espionage Act*, Wash. Post, Nov. 30, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/11/29/AR2010112905973.html (last visited Jan. 3, 2011).

On January 5, 2011, upon motion by the government made at the behest of Twitter,[15] Magistrate Judge Buchanan unsealed the Twitter Order and authorized Twitter to disclose it to its users, including Twitter user [redacted].[16]

In the days following January 5, 2011, the unsealed Twitter Order was posted on the Internet and widely discussed in the media.[17] On January 7, 2011, a "tweet" from Twitter user [redacted] stated that "we can assume Google & Facebook also have secret US government subpoenas."[18]

On January 4, 2011, the day after the government agreed to unseal the Twitter Order, it procured from this Court the Order in this matter, which is substantially identical to the Twitter Order and compels Google to produce the identical information as the Twitter Order for the Google Gmail account [redacted].[19] The perpetual nondisclosure provision in the Order is identical to the Twitter Order nondisclosure provision.

---

[15] Perkins Coie LLP represents both Twitter and Google.

[16] Roche Decl., Ex. 5.

[17] *See, e.g.*, Scott Shane and John F. Burns, *U.S. Subpoenas Twitter Over WikiLeaks Supporters*, N.Y. Times, Jan. 8, 2011, http://www.nytimes.com/2011/01/09/world/09wiki.html (last visited Jan. 13, 2011); Anthony Boadle, *U.S. orders Twitter to hand over Wikileaks records*, Reuters, Jan. 8, 2011, http://www.reuters.com/article/idUSTRE70716420110108 (last visited Jan. 14, 2011).

[18] *See* "ioerror" tweet of Jan. 7, 2011 @ 9:26 p.m. ("Note that we can assume Google & Facebook also have secret US government subpoenas. They make no comment. Did they fold?"), http://twitter.com/ioerror/ (last visited Jan. 18, 2011).

[19] *See* Roche Decl., Ex. 1.

On January 12, 2011, the government issued a preservation request pursuant to 18 U.S.C. § 2703(f) "for the preservation of all stored communications, records, and other evidence" in Google's possession regarding Gmail user [redacted] for November 2009 to the present.[20]

That same day, Google's counsel notified the government that Google wished to immediately give notice of the Order to its user and requested that the government agree to so modify the Order. The government declined this request, saying only that Google is "a different case" from Twitter.[21] The government did however offer to release Google from the notice constraint 90 days after it produced, with a provision allowing the government to petition for a further extension. Google declined this offer and, pursuant to the parties' agreed schedule, filed its motion to modify the Order on January 18, 2011.

On January 26, 2011, three of the users identified in the Twitter Order, including Twitter's [redacted]" user, filed a motion to vacate that order on statutory and Constitutional grounds.[22]

On January 28, 2011, the government filed its response to Google's motion wherein it admitted that the Order and the unsealed Twitter Order relate to the same investigation.[23] The government's brief also established that the targets of their investigation are already operating under the assumption that the government has sought information related to their Google

[20] *Id.*, Ex. 4.

[21] *Id.*, Ex. 7, at 3 n.1.

[22] *Id.*, Ex. 3.

[23] *Id.* Ex. 7, at 3 n.1.

accounts.[24] These facts alone demonstrate that there is no cause for the Order to have been sealed in the first place or to remain sealed now. Moreover, rather than demonstrating how unsealing the Order would harm its well-publicized investigation, the government listed a parade of horribles that have allegedly occurred since it unsealed the Twitter Order, yet failed to establish how any of these developments could be further exacerbated by unsealing this Order.[25]

On February 9, 2011, Magistrate Judge [redacted] denied Google's request to provide immediate notice of the Order to its user.[26] Instead, Magistrate Judge [redacted] authorized Google to provide notice of the Order to the user 90 days after production unless the government obtained a maximum 60-day extension of the non-notification period.[27]

On February 15, 2011, Magistrate Judge [redacted] heard argument on the motion to vacate the Twitter Order, but to Google's knowledge has not yet rendered a decision on that motion.

III. ARGUMENT

A. Standard of Review

Google brings its objections pursuant to Fed. R. Crim. P. 59. *In re U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, Magistrate's No. 07-524M, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008) (objections brought under Rule 59 to magistrate's ruling regarding 2703(d) order)), *vacated on*

[24] *Id.* at Ex. 7 (Exs. 3-4 thereto).

[25] *Id.* at 11-16.

[26] *Id.* Ex. 4.

[27] *Id.*

other grounds by, 620 F.3d 304 (3d Cir. 2010). Because Magistrate Judge [redacted] February 9th ruling on Google's motion to modify the Order is directed to a third party, i.e., Google, it is a dispositive final order. *U.S. v. Myers*, 593 F.3d 338, 345 (4th Cir. 2010) (discovery order directed at a third party is "an immediately appealable final order.") (quoting *Church of Scientology of California v. U.S.*, 506 U.S. 9, 18 n.11 (1992)). Accordingly, the district court must consider Google's objections de novo. *See* Fed. R. Crim. P. 59(b)(3).

B. There is No Need for Secrecy of the Order or the Preservation Request

Nondisclosure orders are permitted in extraordinary circumstances under 18 U.S.C. § 2705. The Order in this matter relies upon the standard set forth in § 2705(b)(5), which provides for nondisclosure when notification will result in "seriously jeopardizing an investigation." Nondisclosure requests such as this are subject to the most demanding scrutiny:

> If the recipients of [surveillance] 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. By constricting the flow of information at its source, the government dries up the marketplace of ideas just as effectively as a customer-targeted injunction would do. Given the public's intense interest in this area of law, such content-based restrictions are subject to rigorous scrutiny.

In re Sealing and Non-Disclosure of Pen/Trap/2703(d) Orders, 562 F. Supp. 2d 876, 882 (S.D. Tex. 2008) (setting a default 180 day period for sealing and non-disclosure of electronic surveillance orders) (internal citations omitted).

Google is not privy to what showing the government made in the affidavit in support of the application for the Order. Given that the government moved to unseal an order to another provider requesting the identical type of information on an account with an identical identifier, it

is difficult to understand how the government could meet the "seriously jeopardizing" standard in this case. The government's offer to release Google from the notice constraint after 90 days demonstrates that a limited nondisclosure provision could have been requested in the first place, and that this very public investigation is at or near an end, which further obviates the need for confidentiality.

Nor does the Order meet the traditional standard for grand jury confidentiality. Grand jury proceedings are traditionally confidential because

> if preindictment proceedings were made public, many prospective witnesses would be hesitant to come forward voluntarily, knowing that those against whom they testify would be aware of that testimony. Moreover, witnesses who appeared before the grand jury would be less likely to testify fully and frankly, as they would be open to retribution as well as to inducements. There also would be the risk that those about to be indicted would flee, or would try to influence individual grand jurors to vote against indictment. Finally, by preserving the secrecy of the proceedings, we assure that persons who are accused but exonerated by the grand jury will not be held up to public ridicule.

Finn v. Schiller, 72 F.3d 1182, 1187 n.6 (4th Cir. 1996) (quoting *Douglas Oil Co. v. Petrol Stops N.W.*, 441 U.S. 211, 219 (1979)). Of course, "it is a 'common-sense proposition that secrecy is no longer "necessary" when the contents of grand jury matters have become public.'" *McHan v. C.I.R.*, 558 F.3d 326, 334 (4th Cir. 2009) (quoting *In re Grand Jury Subpoena*, 438 F.3d 1138, 1140 (D.C. Cir. 2006)).

In this case, the grand jury's investigation of the Twitter user [redacted] is public record. Moreover, Google has preserved all records and content related to the Gmail user [redacted] account. Accordingly, there is no risk of destruction evidence, and none of the other interests served by the traditional secrecy of grand jury proceedings would be undermined in any way by disclosure of this Order or the preservation request.

The government claimed in its response brief before Magistrate Judge [redacted] that unsealing the Order may result in "witness intimidation" in the form of encouraging providers "to resist the government's attempts to gather relevant user information." *See* Government Response, at 16.[28] This argument is specious. First, keeping orders in the shadows to prevent witness intimidation is one thing, but doing so to prevent public discourse is not a proper use of the mechanism. Second, providers are corporate entities advised by competent inside and outside counsel, some of whom are former government attorneys. The notion that these companies could be intimidated into resisting otherwise valid legal process is baseless. Google can only speak for itself, but when it resists legal process, it does so because its attorneys have a good faith belief that the process is deficient or unlawful in some respect, not because Google is trying to curry favor with some interest group. Google has no reason to believe that other providers' approach to legal process is any different.

Additionally, there is no risk of destruction of evidence because Google has preserved responsive information and the Order only demands historical records, not prospective data. The government nevertheless argues that unsealing this Order may cause the targets to "alter[] their modes of communication to evade future investigative efforts," but as the government notes in its brief, the Twitter user [redacted] and other targets of the investigation are already working under the assumption that their Google accounts are the subject of legal process from this grand jury investigation. *See* Government Response, at 14; *see also* Government Exhibits 3-4.[29] Therefore, disclosing this Order will do nothing to alter anyone's behavior, and to the extent [redacted] has already destroyed evidence, unsealing the Order will not reverse those actions either.

The government also claims that the Order must remain sealed "because it might cause

[28] Roche Decl., Ex. 7.

[29] *Id.*

suspects to . . . flee." *See* Government Response, at 13.[30] This argument also fails because if [redacted] is a flight risk, the widespread media coverage of the Twitter Order would have already presumably given him or her and any co-conspirators all the notice they need to start packing their bags, regardless of whether Twitter's [redacted] and Google's [redacted] are one and the same.

Finally, the government asserts that its employees were harassed after the disclosure of the Twitter Order and implies that the same can be expected if this Order is disclosed. *See* Government Response, at 15-16; *see also* Government Exhibit 6.[31] Google condemns any such attacks on government personnel and sympathizes with those forced to endure them. In order to ensure that the same behavior does not occur here, the government should request that the court order any personal identifiers of government personnel redacted before unsealing the Order or preservation letter.

In sum, there is no risk of destruction evidence, and none of the other interests served by the traditional secrecy of grand jury proceedings would be undermined in any way by disclosure of the Order or the preservation request. There is no cause for the Order to remain sealed.

C. The Order May Raise Significant Constitutional and Statutory Issues

As noted, three of the users identified in the Twitter Order, including Twitter's [redacted] user, filed a motion to vacate that order on Constitutional and statutory grounds.[32] In summary, they argued that because the Twitter Order seeks a vast array of information that has no relation to Wikileaks, it could not meet the "specific and articulable facts" standard set forth in 18 U.S.C.

---

[30] *Id.*

[31] *Id.*

[32] Roche Decl., Ex. 3.

§ 2703(d), and that it intrudes upon their First and Fourth Amendment rights for similar reasons.[33] If one assumes for the sake of argument that Twitter's [redacted] and Google's [redacted] are one and the same, it is also reasonable to assume that the user may wish to assert similar objections to this Order. It is therefore within the sound discretion of the Court to modify the Order for the purpose of allowing Google to give notice to its affected user so that the user may decide whether to object to Google's production of the documents and information demanded therein.

D. The Order is a Prior Restraint on Google's Right to Free Speech

The non-disclosure provision in the Order prevents Google from communicating with its user and "is fairly characterized as a regulation of pure speech." *Bartnicki v. Vopper*, 532 U.S. 514, 526 (2001) (referring to Wiretap Act provision prohibiting disclosure of contents of illegally intercepted communication). The Order's non-disclosure provision also prevents Google from defending itself against public criticism such as that cited in the Government's brief. *See* Government Exhibits 3-4. It is of no moment that the person it restrains from speaking, *i.e.*, Google, is a corporate entity. *First Nat'l Bank of Boston v. Bellotti*, 435 U.S. 765, 777 (1978) ("The inherent worth of the speech in terms of its capacity for informing the public does not depend upon the identity of its source, whether corporation, association, union, or individual."). Prior restraints on speech "are constitutionally disfavored in this nation nearly to the point of extinction." *United States v. Brown*, 250 F.3d 907, 915 (5th Cir. 2001). Accordingly, such restraints are subject to the most demanding scrutiny. *In re Sealing and Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 881-82 (S.D. Tex. 2008) ("Prohibiting a service provider from disclosing the existence of the pen/trap or the investigation means that the first-

[33] *Id.*

hand experiences of the recipients of these orders are completely excluded from the public debate" and "dries up the marketplace of ideas just as effectively as a customer-targeted injunction would do.").

Here, Magistrate Judge [redacted] endorsed the government's offer to limit the nondisclosure requirement in the Order to a period of 90 days. While such nondisclosure requirements of a limited duration are not uncommon in normal investigations, this is not a normal investigation. Because the government's interest in ioerror's electronic communications is already so well-publicized and there is absolutely no risk of destruction of evidence, a nondisclosure period of any length is not justified under these circumstances.

IV. CONCLUSION

Google takes no position regarding the propriety of Wikileaks' alleged actions or the government's investigation, but given the extraordinary nature of the issues surrounding the very public Wikileaks investigation, Google requests only that the Court modify the Order to permit notice of the Order and preservation request to be given to Google's user and the user's attorneys. Google further requests that it be permitted to discuss the Order with its user and the user's attorneys and that the user be given 20 days from the date of the Court's order to file an appropriate response. In the meantime, Google has preserved responsive information, and will produce that information if its user does not file a motion or other pleading in opposition within 20 days of the Court's order.

DATED this 17th day of February, 2011.

Respectfully submitted,

By _____

John K. Roche (VSB# 68594)
Perkins Coie LLP
700 13th St., N.W., Suite 600
Washington, D.C. 20005-3960
Phone: 202-434-1627
Fax: 202-654-9106
JRoche@perkinscoie.com

Albert Gidari (*admitted pro hac vice*)
Perkins Coie LLP
1201 Third Avenue, Suite 4800
Seattle, Washington 98101
Phone: 206-359-8000
Fax: 206-359-9000
AGidari@perkinscoie.com

Attorneys for Google Inc.

CERTIFICATE OF SERVICE

I hereby certify that on this 17th day of February, 2011, the foregoing document was sent via hand delivery and email to the following persons:

[redacted]
Assistant United States Attorney
United States Attorney's Office
Eastern District of Virginia
Justin W. Williams United States Attorney's Building
2100 Jamieson Avenue
Alexandria, VA 22314-5794
[redacted]

Attorneys for the United States

By _____
John K. Roche (VSB# 68594)
Perkins Coie, LLP
700 13th St., N.W., Suite 600
Washington, D.C. 20005-3960
Phone: 202-434-1627
Fax: 202-654-9106
JRoche@perkinscoie.com

Attorneys for Google Inc.

ATTACHMENT G

FILED

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

2011 FEB 17 P 3:38

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

IN RE 2703(d) ORDER AND 2703(f) PRESERVATION REQUEST RELATING TO GMAIL ACCOUNT [redacted]	Misc. No. 1:11GJ3794 11-DM-2 FILED UNDER SEAL

GOOGLE INC.'S MOTION TO STAY PRODUCTION PENDING APPEAL OF MAGISTRATE'S ORDER AND MEMORANDUM IN SUPPORT

This matter involves a grand jury investigation of the Wikileaks publication of State Department cables and related matters. The fact of the investigation has been widely reported in the *New York Times* and other news publications, across the Internet and around the globe.[1] Demands have been made to third party service providers, including Google Inc. ("Google"), seeking compelled disclosure of information such as with whom the subject users of those services communicated and which computers they used to do so. The Google Gmail user [redacted] is the subject of such a demand issued by this Court on January 4, 2011 (the "Order").[2] Because of the already public nature of the Wikileaks investigation, and the fact that a nearly identical order to Twitter involving the same account identifier "[redacted] had been unsealed by

[1] *See, e.g.*, Scott Shane and John F. Burns, *U.S. Subpoenas Twitter Over WikiLeaks Supporters*, N.Y. Times, Jan. 8, 2011, http://www.nytimes.com/2011/01/09/world/09wiki.html (last visited Jan. 13, 2011); Anthony Boadle, *U.S. orders Twitter to hand over Wikileaks records*, Reuters, Jan. 8, 2011, http://www.reuters.com/article/idUSTRE70716420110108 (last visited Jan. 14, 2011); Ravi Somaiya, *Release on Bail of WikiLeaks Founder Is Delayed by Appeal*, N.Y. Times, Dec. 14, 2010, *available at* http://www.nytimes.com/2010/12/15/world/europe/15assange.html?src=twrhp (last visited Jan. 3, 2011); *Assange attorney: Secret grand jury meeting in Virginia on WikiLeaks*, CNN Justice, Dec. 13, 2010, http://articles.cnn.com/2010-12-13/justice/wikileaks.investigation_1_julian-assange-wikileaks-case-grand-jury?_s=PM:CRIME (last visited Jan. 3, 2011); Dan Goodin, *Grand jury meets to decide fate of WikiLeaks founder*, The Register, Dec. 13, 2010, *available at* http://www.theregister.co.uk/2010/12/13/assange_grand_jury/ (last visited Jan. 3, 2011).

[2] *See* Declaration of John K. Roche, Ex. 1 ("Roche Decl.").

this Court in the same Grand Jury proceeding ("Twitter Order"),[3] Google filed a motion to modify the Order. Google's motion requested that it be permitted to give notice of the Order to the Gmail user and the user's attorney so they would have a meaningful opportunity to contest the request. Shortly after Google filed its motion, the user identified as "[redacted]" in the Twitter Order filed his own motion to vacate the Twitter Order.[4] That motion was unsealed by this Court and posted on the Internet by the user's attorneys on February 8, 2011.[5] Despite the publicity surrounding the Twitter Order and the related motions, on February 9, 2011, Magistrate Judge [redacted] denied Google's request to provide immediate notice of the Order to its user.[6] Instead, Magistrate Judge [redacted] authorized Google to provide notice of the Order to the user 90 days after production unless the government obtained a maximum 60-day extension of the non-notification period.[7] However, because the government's interest in [redacted] electronic communications is already so well-publicized and there is no risk of destruction of evidence, a nondisclosure period of any length is not justified under these circumstances. Accordingly, Google has today filed its Objections to Magistrate's Order of February 9, 2011 and Notice of Appeal Pursuant to Fed. R. Cr. P. 59.

By this motion, Google requests an order to stay production of documents and information in response to the Order while its concurrently filed Objections are pending. Google respectfully submits that a stay should be granted because, as demonstrated in its Objections, it has made a strong showing of likely success on the merits. Furthermore, Google and its

[3] Roche Decl., Ex. 2

[4] *Id.* Ex. 3.

[5] *See* Electronic Frontier Foundation, *Legal Battle Over Government Demands for Twitter Records Unsealed by Court*, Feb. 8, 2011, http://www.eff.org/press/archives/2011/02/08 (last visited on Feb. 16, 2011).

[6] *Id.* Ex. 4.

[7] *Id.*

subscriber will suffer irreparable injury absent a stay because without a stay the very injury that Google seeks to avoid, production of documents and information without notice to its subscriber, will occur. Furthermore, the issuance of a stay will not injure the government, as it has already agreed to delay production of identical documents and information in response to the Twitter Order and can offer no explanation as to why the documents and information sought by this Order are urgently needed. Google has also preserved the requested records, thus there is no danger of loss or destruction of the information sought. Finally, the issuance of a stay is in the public's interest because the public can have no interest in the enforcement of an unjustified nondisclosure provision and a stay will ensure that the user is afforded an opportunity to assert any Constitutional or statutory rights he or she may have with regard to the Order.

The pertinent factual background is set forth in Google's Objections to Magistrate's Order of February 9, 2011 and Notice of Appeal Pursuant to Fed. R. Cr. P. 59, which were also filed today. Rather than burden the Court with a duplicative recitation of facts, that factual background is expressly incorporated herein.

I. ARGUMENT

A. Standard of Review

The court's decision whether to grant a stay pending appeal is governed by four factors: 1) whether the stay applicant has made a strong showing of likely success on the merits; 2) whether the applicant will suffer irreparable injury absent a stay; 3) whether issuance of a stay will injure other parties to the proceeding; and 4) how issuance of a stay will affect the public interest. *U.S. v. Dyer*, 750 F. Supp. 1278, 1299 n.40 (E.D. Va. 1990).

B. **The Court Should Grant a Stay of Production Pending Google's Appeal**

1. **Google Has Made a Strong Showing of Likely Success on the Merits**

As set forth in Google's Objections to Magistrate's Order of February 9, 2011 and Notice of Appeal Pursuant to Fed. R. Cr. P. 59, Google is likely to succeed on the merits because the government's investigation of Wikileaks generally, and its interest in the [redacted] user name specifically, is a matter of public record, thus obviating the need for the Order's nondisclosure provision. Furthermore, the Order, like the Twitter Order, may present substantial Constitutional and statutory concerns that the user may wish to raise before this Court. Additionally, given that the Order's nondisclosure provision is a prior restraint on Google's First Amendment right to communicate with its users, a nondisclosure period of any length is not justified under these circumstances. Finally, Google has preserved the requested records, thus there is no danger of loss or destruction of the information sought. Accordingly, Google respectfully submits it has a strong likelihood of success on the merits.

2. **Google and its User Will Suffer Irreparable Injury Absent a Stay**

Google brings its objections in order to provide its user with the opportunity to assess whether the Order, like the Twitter Order, presents substantial constitutional and statutory issues that the user may wish to raise before this Court. If Google must comply with the Order before a ruling is issued on its Objections, the government will have obtained the very information that the user may seek to protect before the user ever has an opportunity to object. Hence, the government will have gotten the documents and information it seeks, and any knowledge derived therefrom cannot simply be erased from the minds of the government's lawyers even if the user were to subsequently prevail on appeal once he or she eventually receives notice of the Order. *Maness v. Meyers*, 419 U.S. 449, 460 (1975) ("Compliance could cause irreparable injury

because appellate courts cannot always 'unring the bell' once the information has been released."); *In re Grand Jury Proceedings*, 601 F.2d 162, 169 (5th Cir. 1979) (*Maness* rule may apply to pre-trial proceedings and surrender of non-constitutional rights or privileges). Moreover, "the Supreme Court has explained that 'loss of First Amendment freedoms, for even minimal periods of time, unquestionably constitutes irreparable injury.'" *Newsom ex rel. Newsom v. Albemarle County School Bd.*, 354 F.3d 249, 261 (4th Cir. 2003) (quoting *Elrod v. Burns*, 427 U.S. 347, 373 (1976). Therefore, to the extent the Court foresees any possibility that the Order impinges on Google's or its users First Amendment rights, those rights will suffer irreparable injury absent a stay.

3. A Stay Will Not Injure the Government

The issuance of a stay will not injure the government, as it has already agreed to delay production of identical documents and information in response to the Twitter Order and can offer no explanation as to why the documents and information sought by this Order are urgently needed. Indeed, the government filed a motion to delay the hearing on Google's original motion until after Judge Buchanan had an opportunity to rule on the Twitter Order. Moreover, to the extent the Court agrees that Google is likely to succeed on the merits of its claim, the government cannot suffer any harm from a stay pending appeal. *Newsom*, 354 F.3d at 261 (appellee suffered no harm by issuance of an injunction preventing it from enforcing a regulation that was likely to be found unlawful). Finally, Google has preserved the requested records, thus there is no danger of loss or destruction of the information sought if the Order is stayed.

4. Issuance of a Stay Will Serve the Public Interest

The issuance of a stay is in the public's interest because the public can have no interest in the enforcement of a nondisclosure provision where the underlying grand jury investigation and

the government's interest in the electronic communications of the [redacted] user name are so public. *McHan v. C.I.R.*, 558 F.3d 326, 334 (4th Cir. 2009) (quoting *In re Grand Jury Subpoena*, 438 F.3d 1138, 1140 (D.C. Cir. 2006)) ("it is a 'common-sense proposition that secrecy is no longer "necessary" when the contents of grand jury matters have become public.'"). Furthermore, a stay will ensure that the user is afforded an opportunity to assert any Constitutional or statutory rights he or she may have with regard to the Order. *Newsom*, 354 F.3d at 261 ("Surely, upholding constitutional rights serves the public interest.").

II. CONCLUSION

For the reasons stated, Google requests an order to stay production of documents and information in response to the Order while its concurrently filed Objections are pending.

DATED this 17th day of February, 2011.

Respectfully submitted,

By _____

John K. Roche (VSB# 68594)
Perkins Coie LLP
700 13th St., N.W., Suite 600
Washington, D.C. 20005-3960
Phone: 202-434-1627
Fax: 202-654-9106
JRoche@perkinscoie.com

Albert Gidari (*pro hac vice pending*)
Perkins Coie LLP
1201 Third Avenue, Suite 4800
Seattle, Washington 98101
Phone: 206-359-8000
Fax: 206-359-9000
AGidari@perkinscoie.com

Attorneys for Google Inc.

CERTIFICATE OF SERVICE

I hereby certify that on this 17th day of February, 2011, the foregoing document was sent via hand delivery and email to the following persons:

[redacted]
Assistant United States Attorney
United States Attorney's Office
Eastern District of Virginia
Justin W. Williams United States Attorney's Building
2100 Jamieson Avenue
Alexandria, VA 22314-5794
[redacted]

Attorneys for the United States

By _____
John K. Roche (VSB# 68594)
Perkins Coie, LLP
700 13th St., N.W., Suite 600
Washington, D.C. 20005-3960
Phone: 202-434-1627
Fax: 202-654-9106
JRoche@perkinscoie.com

Attorneys for Google Inc.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

IN RE 2703(d) ORDER AND 2703(f) PRESERVATION REQUEST RELATING TO GMAIL ACCOUNT [redacted]	Misc. No. 10GJ3793 11-DM-2 FILED UNDER SEAL

DECLARATION OF JOHN K. ROCHE IN SUPPORT OF GOOGLE INC.'S OBJECTIONS TO MAGISTRATE'S ORDER OF FEBRUARY 9, 2011 AND NOTICE OF APPEAL PURSUANT TO FED. R. CRIM. P. 59 AND MOTION TO STAY PRODUCTION PENDING APPEAL OF MAGISTRATE'S ORDER

I, John K. Roche, declare as follows:

1. I am an attorney licensed to practice in the Commonwealth of Virginia and the District of Columbia, and am admitted to practice before this Court. I am an associate in the law firm of Perkins Coie LLP, counsel of record for Google Inc. ("Google") in this action. As one of the attorneys with responsibility for the representation of Google in this matter, I have personal knowledge of the facts set forth below and am competent to testify about the matters stated herein.

2. Attached hereto as Exhibit 1 is the January 4, 2011 order of this Court issued to Google pursuant to 18 U.S.C. § 2703(d) (the "Order") in the above-referenced matter.

3. Attached hereto as Exhibit 2 is the December 14, 2010 order of this Court issued to Twitter pursuant to 18 U.S.C. § 2703(d) (the "Twitter Order") in the above-referenced matter.

4. Attached hereto as Exhibit 3 is the January 26, 2011 Motion of Real Parties in Interest Jacob Appelbaum, Birgitta Jonsdottir, and Rop Gonggrijp to Vacate December 14, 2010 Order.

5. Attached hereto as Exhibit 4 is the February 9, 2011 Order Granting in Part and Denying in Part Google's Motion to Modify 2703(d) Order for the Purpose of Providing Notice to User.

6. Attached hereto as Exhibit 5 is the January 5, 2011 order of this Court unsealing the Twitter Order.

7. Attached hereto as Exhibit 6 is the January 12, 2011 preservation request issued to Google pursuant to 18 U.S.C. § 2703(f) in the above-referenced matter.

8. Attached hereto as Exhibit 7 is the Response of the United States to Google's Motion to Modify 2703(d) Order for the Purpose of Providing Notice to User.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed this 17th day of February, 2011.

John K. Roche

CERTIFICATE OF SERVICE

I hereby certify that on this 17th day of February, 2011, the foregoing document was sent via hand delivery and email to the following persons:

[redacted]
Assistant United States Attorney
United States Attorney's Office
Eastern District of Virginia
Justin W. Williams United States Attorney's Building
2100 Jamieson Avenue
Alexandria, VA 22314-5794
[redacted]

Attorneys for the United States

By _____
John K. Roche (VSB# 68594)
Perkins Coie, LLP
700 13th St., N.W., Suite 600
Washington, D.C. 20005-3960
Phone: 202-434-1627
Fax: 202-654-9106
JRoche@perkinscoie.com

Attorneys for Google Inc.

EXHIBIT 1

U.S. Department of Justice

United States Attorney

Eastern District of Virginia

Justin W. Williams United States Attorney's Building
2100 Jamieson Avenue
Alexandria, Virginia 22314-5794
(703) 299-3700

FACSIMILE TRANSMISSION COVER PAGE

DATE: 1/5/11

TO: Google, Inc

PHONE: Attn: Custodian of Records

TO FAX NO.: (650) 649-2939 / (650) 249-3429

SENDER: [redacted] Assistant to [redacted]

SENDER'S PHONE NO.: (703) 299 [redacted]

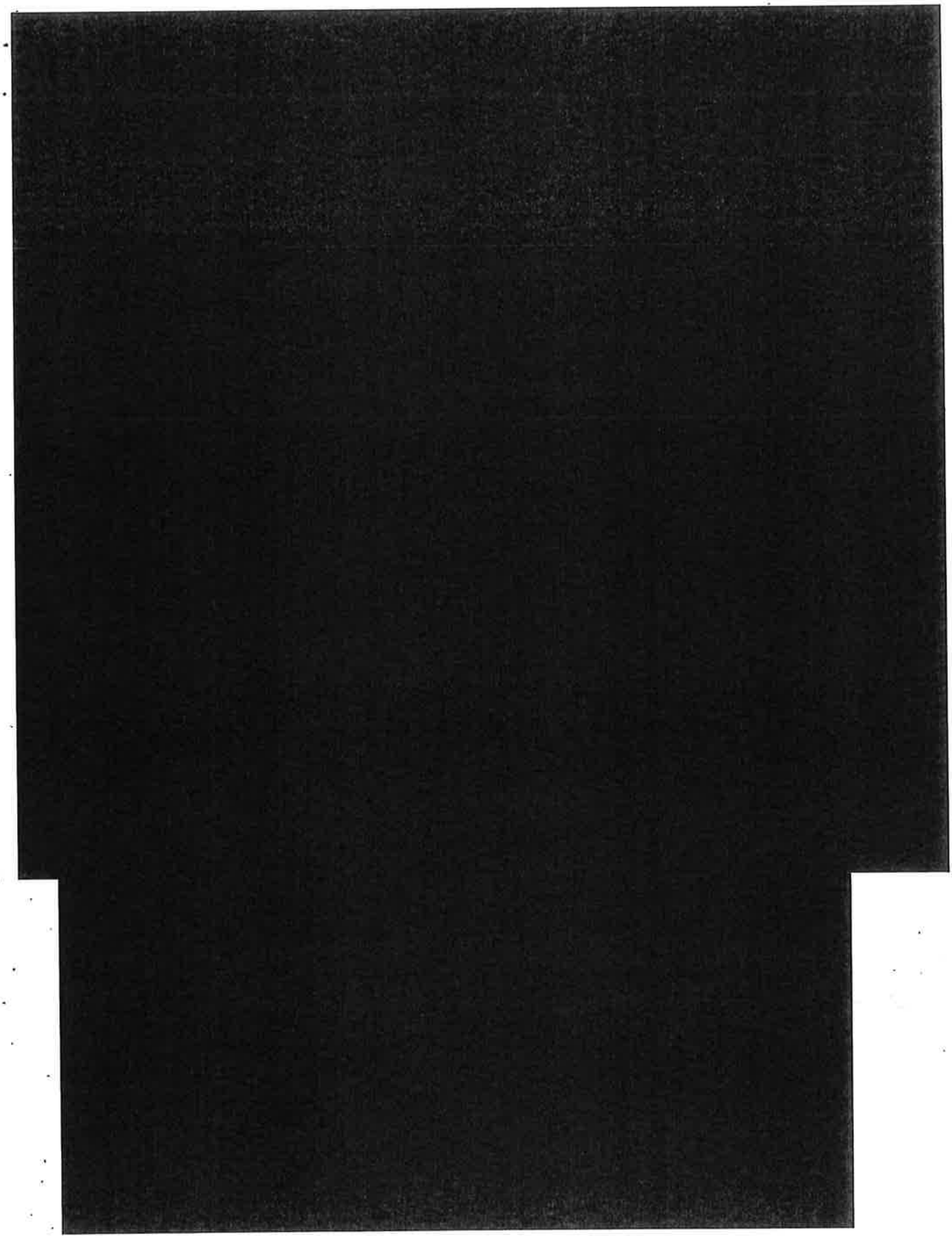
SENDER'S FAX NO.: (703) 299 [redacted]

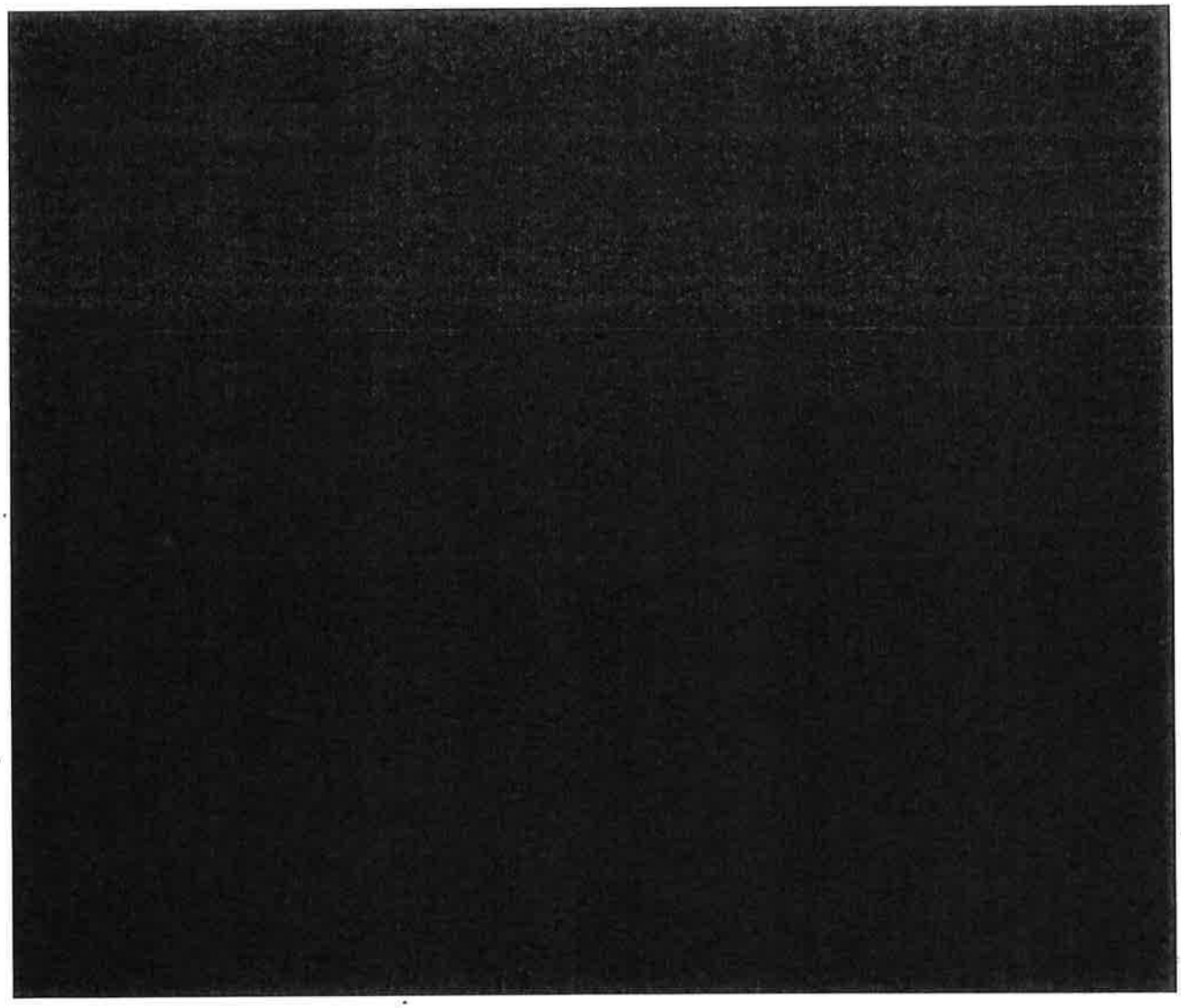
NUMBER OF PAGES: 3 *Not Including Cover Page*

Level of Transmitted Information:

- ☐ **Non-Sensitive Information**
- ☑ **Sensitive But Unclassified (SBU)**
- ☐ **Limited Official Use (LOU)**
- ☐ **Grand Jury Information**
- ☐ **Tax Information**
- ☐ **Law Enforcement Information**
- ☐ **Victim Witness Information**

CONTENTS:





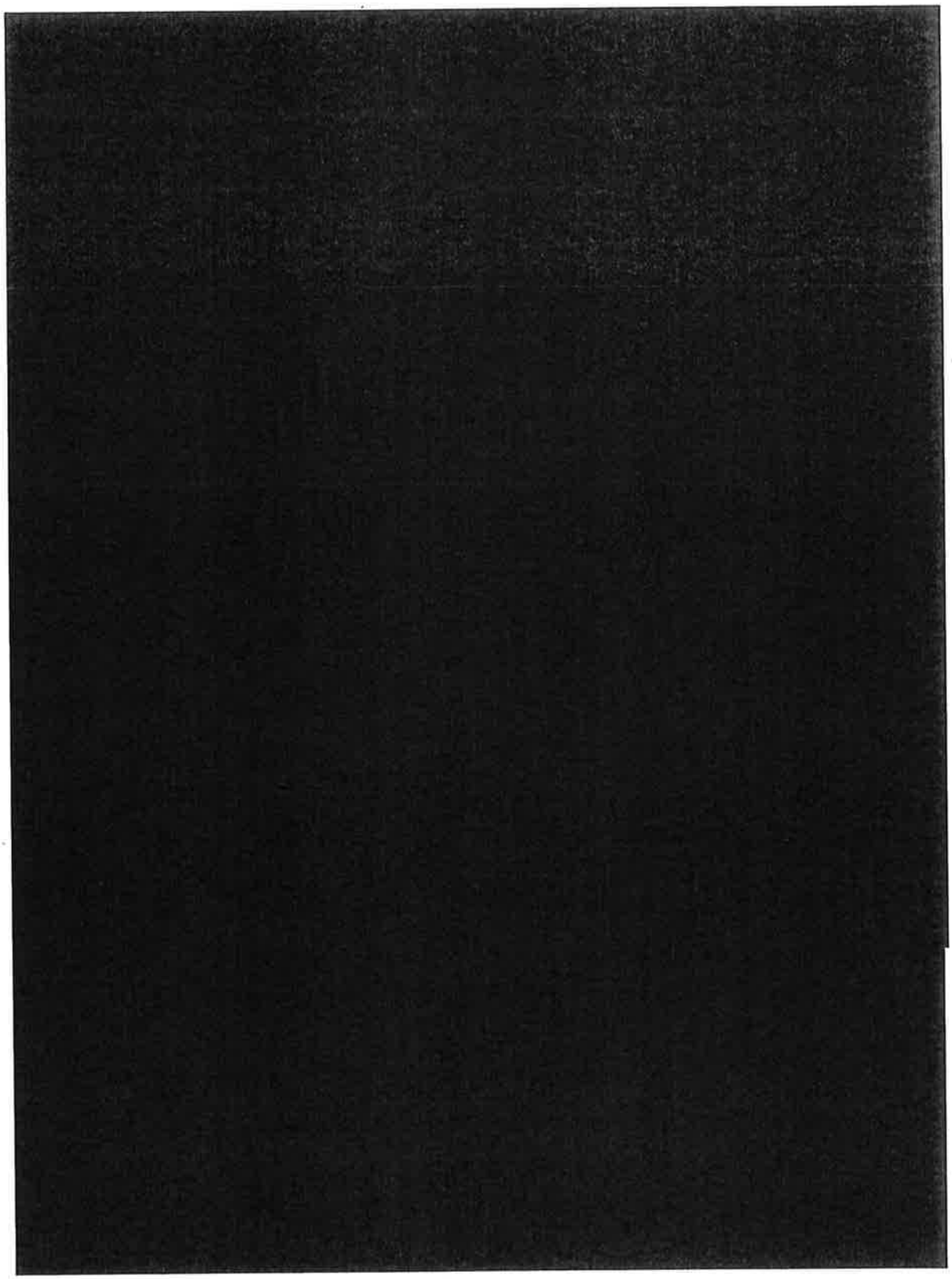


EXHIBIT 2

U.S. Department of Justice

United States Attorney

Eastern District of Virginia

Justin W. Williams United States Attorney's Building
2100 Jamieson Avenue
Alexandria, Virginia 22314-5794
(703) 299-3700

FACSIMILE TRANSMISSION COVER PAGE

DATE: 12/14/10

TO: Twitter Attn: Trust & Safety

PHONE:

TO FAX NO.: (415) 222-9958

SENDER: [redacted] Assistant to [redacted]

SENDER'S PHONE NO.: 703 299 [redacted]

SENDER'S FAX NO.: 703 299 [redacted]

NUMBER OF PAGES: 4 *Not Including Cover Page*

Level of Transmitted Information:

- ☐ **Non-Sensitive Information**
- ☐ **Sensitive But Unclassified (SBU)**
- ☒ **Limited Official Use (LOU)**
- ☐ **Grand Jury Information**
- ☐ **Tax Information**
- ☐ **Law Enforcement Information**
- ☐ **Victim Witness Information**

CONTENTS:

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)	MISC. NO. 10GJ3793 Filed Under Seal

ORDER

This matter having come before the Court pursuant to an application under Title 18, United States Code, Section 2703, which application requests the issuance of an order under Title 18, United States Code, Section 2703(d) directing Twitter, Inc., an electronic communications service provider and/or a remote computing service, located in San Francisco, California, to disclose certain records and other information, as set forth in Attachment A to this Order, the Court finds that the applicant has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation.

IT APPEARING that the information sought is relevant and material to an ongoing criminal investigation, and that prior notice of this Order to any person of this investigation or this application and Order entered in connection therewith would seriously jeopardize the investigation;

IT IS ORDERED pursuant to Title 18, United States Code, Section 2703(d) that Twitter, Inc. will, within three days of the date of this Order, turn over to the United States the records and other information as set forth in Attachment A to this Order.

IT IS FURTHER ORDERED that the Clerk of the Court shall provide the United States Attorney's Office with three (3) certified copies of this application and Order.

IT IS FURTHER ORDERED that the application and this Order are sealed until otherwise ordered by the Court, and that Twitter shall not disclose the existence of the application or this Order of the Court, or the existence of the investigation, to the listed subscriber or to any other person, unless and until authorized to do so by the Court.

[redacted]
United States Magistrate Judge

12/14/10
Date

A TRUE
CLERK, U.S. COURT
[redacted]
BY: DEPUTY CLERK

ATTACHMENT A

You are to provide the following information, if available, preferably as data files on CD-ROM, electronic media, or email [redacted] r otherwise by facsimile to [redacted]

A. The following customer or subscriber account information for each account registered to or associated with [redacted] e time period November 1, 2009 to present:

1. subscriber names, user names, screen names, or other identities;
2. mailing addresses, residential addresses, business addresses, e-mail addresses, and other contact information;
3. connection records, or records of session times and durations;
4. length of service (including start date) and types of service utilized;
5. telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
6. means and source of payment for such service (including any credit card or bank account number) and billing records.

B. All records and other information relating to the account(s) and time period in Part A, including:

1. records of user activity for any connections made to or from the Account, including the date, time, length, and method of connections, data transfer volume, user name, and source and destination Internet Protocol address(es);
2. non-content information associated with the contents of any communication or file stored by or for the account(s), such as the source and destination email addresses and IP addresses.
3. correspondence and notes of records related to the account(s).

EXHIBIT 3

UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF VIRGINIA

ALEXANDRIA DIVISION

IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)	MISC NO. GJ3793 **ORAL ARGUMENT REQUESTED**

MOTION OF REAL PARTIES IN INTEREST JACOB APPELBAUM, BIRGITTA JONSDOTTIR, AND ROP GONGGRIJP TO VACATE DECEMBER 14, 2010 ORDER

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Federal Cases

State Cases

Federal Statutes

Federal Rules

Constitutional Provisions

Other Authorities

I. INTRODUCTION

Real parties in interest Jacob Appelbaum, Birgitta Jonsdottir, and Rop Gonggrijp (collectively "Parties") hereby move to vacate the Court's December 14, 2010 Order requiring Twitter, Inc. to disclose extensive information related to their private Twitter accounts pursuant to section 2703(d) of the Stored Communications Act, 18 U.S.C. § 2701 *et seq.* ("December 14 Order" or "Order"). There is no reasonable basis for the Order and the Court should vacate it for the following reasons.

First, the face of the December 14 Order demonstrates that the government's *ex parte* Application purportedly "showing that there are reasonable grounds" for the Order likely contains material errors or omissions that render the Application insufficient.[1] The face of the December 14 Order indicates that the government's underlying investigation presumably relates, in some way, to the website WikiLeaks. Under 18 U.S.C. § 2703(d), therefore, any application must provide "specific and articulable facts" showing that the Parties' Twitter information sought is both "relevant" and "material" to an on-going investigation about WikiLeaks. No such "specific and articulable facts" could have been provided here, however, because the government has sought information about all of the Parties' Twitter-related publications and speech over a 6 ½ month period of time and all of the Parties' Twitter-based direct messages between themselves and certain others, even though the vast majority of that information has nothing to do with WikiLeaks at all. As such, non-WikiLeaks-related information cannot be relevant or material to a WikiLeaks-related investigation and the government's Application cannot have provided the specific facts needed to justify a proper § 2703 order.

Second, the Order intrudes upon important First Amendment rights. It is impermissibly overbroad because it demands production of information that will not directly further the government's purported interests. Moreover, to the extent that the Parties' Twitter accounts are subject to government snooping because of what the Parties have said and because of who they

[1] As detailed further below, the government's refusal to provide the Parties with its Application, therefore denying the Parties an opportunity to respond directly to its assertions, does not prevent the Parties from challenging these problems because courts have long recognized the right to challenge third-party production demands—even where the request is cloaked in secrecy. In light of this secrecy, the Parties have filed a companion Motion to Unseal the Application. If the Court orders disclosure of such materials, the Parties will supplement this Motion.

know, that it impermissable. They each spoke on Twitter about what has become a political cause, *i.e.*, the WikiLeaks website and its founder Julian Assange. But, the First Amendment guarantees their right to speak up for and freely associate with even unpopular people and causes. Where a disclosure demand implicates First Amendment freedoms, it must be scrutinized with special care and governmental fishing expeditions that improperly intimidate and silence cannot survive First Amendment scrutiny.

Third, the Order threatens the Parties' Fourth Amendment rights because disclosure could reveal that the Parties were located in particular private spaces at particular times—information in which they maintain a reasonable expectation of privacy. The government cannot track movements and location that may reveal intimate details of a person's life without the safeguards of a valid warrant based on probable cause.

Fourth, because the Order and Application raise serious constitutional concerns, the Court should exercise its discretion under § 2703(d) to require the government to obtain a warrant based on probable cause. The Court should exercise this discretion here to avoid the constitutional questions raised by warrantless disclosure and ensure that the Parties' rights are not improperly trampled.

Finally, the demand for information about Ms. Jonsdottir—a Member of the Icelandic Parliament—is contrary to Icelandic law and creates a disturbing precedent regarding a foreign government's ability to collect private data from another country's officials.

When Congress amended the Stored Communications Act in 1994, it emphasized the need to "guard against 'fishing expeditions' by law enforcement." *See* H.R. Rep. No. 103-827, at 31-32 (1994), *reprinted in* 1994 U.S.C.A.A.N. 3489, 3511-12. Here, the Court should do just that by vacating the December 14 Order and denying the government's Application for records related to the Twitter accounts associated with "rop_g"; "ioerror," and "birgittaj."

II. BACKGROUND

On December 14, 2010, this Court entered a sealed order directing Twitter, Inc. to provide the government with records and other information related to the accounts of several of

its users, including the Parties here. Sears Decl.,[2] Exh. 1 (the "Dec. 14 Order"). On January 5, 2011, the Court unsealed the Order. Sears Decl., Exh. 2. Twitter informed the Parties of the record demand two days later. *See, e.g.*, Sears Decl., Exh. 3.

The Parties' Motion for Unsealing of Sealed Court Records, filed concurrently, provides a detailed factual and procedural background. The Parties incorporate that discussion by reference rather than repeat it here. *See* Motion for Unsealing of Sealed Court Records at 4-6.

In sum, the December 14 Order requires Twitter to provide the government with records related to the Parties' Twitter accounts —including home addresses, connection records, and Internet Protocol addresses.[3] *See* Exh. 1 (Dec. 14 Order at Attach. A). Twitter is an on-line communications tool that permits users to express their thoughts in individual messages ("Tweets") of 140 characters or less. *See* Motion to Unseal at 4-6; *see also* http://twitter.com/about. The heart of the service is short, public text messages that express opinions, relate thoughts, and provide commentary. Users can also provide links to other websites (if space permits), "re-tweet" (i.e., re-publish) Twitter messages made by others, and send direct messages to other users.

Here, all three Parties—Jacob Appelbaum, Birgitta Jonsdottir, and Rop Gonggrijp—have public Twitter feeds they use to express opinion and share commentary on public events and issues. Anyone can read their Tweets at the Twitter website and anyone can sign up to follow the Parties' Twitter feeds. Each of the Parties uses Twitter extensively and/or has thousands of "followers" who follow what they post.

On its face the Dec. 14 Order seeks information about all of those who received the Parties' publications and private messages, mapping their associations and audience. Even after the actual information to be produced under the Order was narrowed by the government pursuant to concerns raised by Twitter,[4] it requires Twitter to disclose such information for all of the

---

[2] Declaration of Stuart Sears In Support of Motion Of Real Parties In Interest Jacob Appelbaum, Birgitta Jonsdottir, and Rop Gonggrijp to Vacate December 14. 2010 Order (hereinafter "Sears Decl.").

[3] An Internet Protocol ("IP") address is a unique numerical address that identifies individual computers or other devices as they interact over the Internet. *See infra* at III.C.

[4] The government has not conceded that its original Order was improper in any manner. Nor has the government agreed never to ask for the full scope of the originally demanded information.

Parties' Twitter-related speech (called "Tweets") for multiple months, *i.e.*, November 15, 2009 to June 1, 2010, regardless of any connection between the postings and WikiLeaks. Such information is also requested for all of the Parties' Twitter-based direct messages between each other during the same multi-month time period—again, regardless of any connection between the messages and WikiLeaks. The Order's breadth is significant because each of the Parties use Twitter extensively and/or have thousands of "followers" who follow what they post – as of January 25, 2011, Mr. Appelbaum has posted 7,909 Tweets and has 10,699 followers, Ms. Jonsdottir has posted 1211 Tweets and has 5,904 followers, and Mr. Gonggrijp has posted 77 Tweets and has 4223 followers. Mr. Appelbaum, Ms. Jondottir and Mr. Gongrijp have also all published many Twitter messages that are wholly unrelated to WikiLeaks, including tweets which comment on the political situations in Tibet and Tunisia, comment on the Icelandic volcano that blanketed Europe with ash in 2010, or address issues such as the TSA, obscenity and gay marriage laws, and charitable causes. *See* Sears Decl. Exh. 4 (examples of the Parties' non-WikiLeaks related Twitter postings). Thus, the Application and Order must be viewed for what they are—an improper and overbroad fishing expedition.

III. ARGUMENT

A. No "specific and articulable facts" exist to show that the information sought is "relevant and material" to an ongoing criminal investigation.

To obtain an order to disclose customer records under the Stored Communications Act, the government must provide "specific and articulable facts showing that there are reasonable grounds to believe that the ... records or information sought[] are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d) (emphasis added). In the December 14 Order, the Court found that it appeared "that the information sought is relevant and material to an ongoing criminal investigation" and granted the disclosure request. The Court, however, was constrained in its consideration at that time because it had before it only the government's Application for the section 2703(d) disclosure order. The Parties believe the government's Application must contain material errors or omissions because there can be no reasonable basis

---

As a result, Movants' challenge to the December 14 Order need not be limited to the narrowed demand.

for finding that the information sought here regarding the Parties' Twitter accounts is both "relevant" and "material" to an ongoing investigation.

Section 2703's "specific and articulable" fact standard requires more than mere suspicion to justify a disclosure order. Even in the context of an investigative stop based on suspected illegality, the government cannot simply rely upon an "inchoate and unparticularized suspicion or hunch," but instead must demonstrate specific facts regarding possible illegal conduct to justify a stop. *See, e.g., Terry v. Ohio*, 392 US 1, 27 (1968); *United States v. Jones*, 242 F.3d 215, 217 (4th Cir. 2001) (finding that the "specific and articulable" standard forbids reliance on suspicions or hunches and therefore rejecting a search based upon an uncorroborated tip); *United States v. Brignoni-Ponce*, 422 US 873, 882, 884-85 (1975) (rejecting a search based upon one factor, the defendant's race, because the reasonableness requirement demands more than "broad and unlimited discretion" and instead requires specific facts demonstrating reasons to believe that potential illegal conduct may be occurring). Here, however, the government is reaching beyond a simple investigative stop and is broadly seeking non-public information regarding the Parties' protected Twitter-based speech and associational contacts. At a minimum, therefore, the government must be required to articulate "specific and articulable facts" that do more than speculate about a nexus between the specific information sought and the potential targets of the government's WikiLeaks-related investigation.

Section 2703 also requires the government to meet its materiality requirement before any order may issue. In a number of contexts, the United States Supreme Court and the Fourth Circuit have emphasized that a showing of materiality requires more than mere theoretical relevance. To establish materiality, the party seeking disclosure must establish through more than mere speculation that the information is, *i.e.*, "vital" or "highly relevant" to the inquiry or "helpful" or "essential" to the party's position. *See, e.g., United States v. Valenzuela-Bernal*, 458 U.S. 858, 867-73 (1982) (access to evidence); *Roviaro v. United States*, 353 U.S. 53, 62-65 (1957) (disclosure of informant's identity); *United States v. Smith*, 780 F.2d 1102, 1109 (4th Cir. 1985) (*en banc*) (standard for overcoming classified information privilege).

Tellingly, the Government refuses to provide its Application to the Parties so that the

Parties may directly challenge the Government's statements seeking to justify the search.[5] But, whatever the Application may claim, it cannot tell the whole story and cannot establish that the information sought in this Order is both "relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d) (emphasis added). Indeed, although the face of the December 14 Order suggests that this investigation relates to WikiLeaks[6], the Order requires Twitter to provide the government with records related to thousands of the Parties' "Tweets" over many months that have nothing whatsoever to do with WikiLeaks. The Parties Tweets about issues such as the political situations in Tibet and Tunisia, a volcano in Iceland, the TSA obscenity and gay marriage laws and charitable cases are not relevant to the government's purported investigative purpose—and they certainly cannot be vital or essential to the government's investigation into WikiLeaks.

Moreover, despite the fact that the Parties' Twitter messages cover a broad range of non-WikiLeaks topics, the government wants private information related to the Parties' accounts, all their Tweets and all their direct messages to each other and certain others during the relevant time period—even information that the Parties do not choose to share with the world. This includes the Internet Protocol address ("IP address") information related to each time the Parties logged into Twitter over a 6 ½ month period of time, the IP address information related to the Parties' direct messages to themselves and certain others, and the date and time information related to all the Parties' log ins and direct messages over this multi-month time period. This Order requires production of this information for all the Parties' Tweets and direct messages during a multi-month time period, without regard to whether the messages relate to WikiLeaks or any other specific subject.

In light of the Order's mandate to produce a broad swath of data that has no connection

---

[5] The Parties have filed a companion Motion to Unseal the Application and will supplement this Motion if the Court orders disclosure. Even if the Application is not unsealed, it should be disclosed to the Parties under seal so they can fairly challenge the December 14 Order and address the government's statements directly on Reply.

[6] Press reports issued after the Order became public confirm this WikiLeaks connection. *See, e.g.*, *Scott Shane and John F. Burns, U.S. Subpoenas Twitter Over WikiLeaks Supporters*, N.Y. Times, Jan. 9, 2011, at A1 *available at* http://www.nytimes.com/2011/01/09/world/09wiki.html; David Batty, *US Orders Twitter To Hand Over WikiLeaks Members' Private Details, The Guardian, Jan. 8, 2011.*

whatsoever to WikiLeaks and cannot be relevant or material to any investigation, the December 14 Order should be vacated, the Application disclosed, and the Parties afforded a fair opportunity to further challenge the Government's assertions and highlight any material misstatements or omissions in the Application. *See Franks v. Delaware*, 438 U.S. 154, 169 (1978).

B. The Order Should be Vacated Because it Intrudes Upon the Parties' First Amendment Rights.

On its face, the Order threatens the Parties' protected First Amendment rights. The Parties' Twitter-related activities are core protected conduct and speech is entitled to the highest level of First Amendment protection. *See, e.g., Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969) ("the constitutional guarantees of free speech and free press do not permit the State to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action"); *Hess v. Indiana*, 414 U.S. 105, 108-109 (1973) (the state may not criminalize advocacy of the use of force or law-breaking unless the charged conduct is "intended to produce, and likely to produce, *imminent* disorder") (emphasis in original)).

The Supreme Court's holding in *Virginia v. Black*, 538 U.S.343 (2003), illustrates the sanctity of speech. The Court emphasized that the government may not prohibit "dissemination of social, economic and political doctrine"—even that "which a vast majority of its citizens believes to be false and fraught with evil consequence." *Id.* at 358 (citation omitted). Even distasteful and threatening gatherings and speeches are protected in our democracy. *Brandenburg*, 395 U.S. at 447. As the Court explained in *Brandenburg*, efforts to "punish mere advocacy and to forbid, on pain of criminal punishment, assembly with others merely to advocate the described type of action" violate the First Amendment. *Id.* at 449.

Moreover, freedom of association even with unpopular individuals and groups is an inseparable aspect of Constitutional "liberty." *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 460 (1958) ("It is beyond debate that freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the 'liberty' assured by the Due Process Clause of the Fourteenth Amendment which embraces freedom of speech."). Indeed, "[t]he right to associate in order to express one's views is 'inseparable' from the right to speak freely." *Cromer*

v. Brown, 88 F.3d 1315, 1331 (4th Cir. 1994) (citation omitted). As the Fourth Circuit explained, "we have long understood as implicit in the right to engage in activities protected by the First Amendment a corresponding right to associate with others in pursuit of a wide variety of political, social, economic, educational, religious, and cultural ends." *Id.* (quoting *Roberts v. U.S. Jaycees*, 468 U.S. 609, 622 (1984)); *see also Shelton v. Tucker*, 364 U.S. 479, 486 (1960) ("the right of free association is a right closely allied to freedom of speech and a right which, like free speech, lies at the foundation of a free society").

Here, the government has declared its disapprobation of WikiLeaks and its desire to prosecute somebody associated with it. Attorney General Holder personally proclaimed that the government will prosecute anyone it can and that the Department of Justice's tough talk "is not saber-rattling." *See* Pete Yost, Assoc. Press, *Holder says Wikileaks under investigation*, http://news.yahoo.com/s/ap/20101129/ap_on_go_ca_st_pe/us_wikileaks_holder (Last visited on Jan. 25, 2011). But, no matter how much the Government dislikes any given speech or advocacy, it cannot use that protected conduct as a pretext for searches or a basis for criminality.[7]

The Government's fishing expedition into information about all the Parties' Twitter postings, and about certain of the Parties' direct messages, over a 6 ½ month time period may chill the Parties' and other individuals' rights to speak freely and associate with others. Such governmental efforts that chill expression must be analyzed with particular scrutiny. *North Carolina Rt. To Life v. Bartlett*, 168 F.3d 705, 715 (4th Cir. 1999). Moreover, where "an investigation ... intrudes into the area of constitutionally protected rights of speech, press, association and petition," the government must "convincingly show a substantial relation between the information sought and a subject of overriding and compelling state interest." *Gibson v. Fla. Legislative Invest. Comm.*, 372 U.S. 539, 546 (1963); *see also In re Grand Jury Subpoenas Duces Tecum.*, 78 F.3d 1307, 1312 (8th Cir. 1996) ("A grand jury subpoena will be

[7] Even where an organization is alleged to have illegitimate aims, the government may not paint all supporters or advocates with a broad brush, ignoring the particulars behind each individual's speech, association, and intent. Rather, the actions of persons accused of improperly supporting such groups "must be judged *strictissimi juri*, for otherwise there is a danger that one in sympathy with the legitimate aims of the organization, but not specifically intending to accomplish them by resort to violence, might be punished for his adherence to lawful and constitutionally protected purposes, because of other unprotected purposes which he does not necessarily share." *Noto v. United States*, 367 U.S. 290, 299-300 (1961).

enforced despite a First Amendment challenge if the government can demonstrate a compelling interest in and a sufficient nexus between the information sought and the subject matter of its investigation."); *In re First Na"l Bank*, 701 F.2d 115, 119 (10th Cir. 1983) ("If the district court determines that enforcement of the subpoena would likely chill associational rights, the Government must show a compelling need"). As the Supreme Court has cautioned, "justifiable governmental goals may not be achieved by unduly broad means having an unnecessary impact on protected rights of speech, press, or association." *Branzburg v. Hayes*, 408 U.S. 665, 680-81 (1972).

Courts have long recognized individuals' right to challenge disclosure demands that implicate First Amendment freedoms and reviewed such demands with special care. *See, e.g.*, *Eastland v. U.S. Servicemen's Fund*, 421 U.S. 491, 501 n.14 (1975) (individuals must have right to challenge third-party subpoena for their records or unconstitutional intrusions could go unchallenged); *Pollard v. Roberts*, 283 F. Supp. 248, 258-59 (E.D. Ark. 1968) (three-judge court), *aff'd* per curiam, 393 U.S. 14 (1968) (enjoining subpoenas directed at third-party bank because enforcement would violate customer's First Amendment rights of association); *In re First Nat'l Bank*, 701 F.2d at 117-19 (remanding for evidentiary hearing on claims that government's compulsion of information from third parties would violate target's First Amendment right of association); *Local 1814, Int'l Longshoremen's Ass'n v. Waterfront Comm'n of N.Y. Harbor*, 667 F.2d 267, 271, 274 (2d Cir. 1981) (upholding district court's decision to narrow third-party subpoena to limit impairment of targets' First Amendment rights of association).[8]

Here, the government's Application and the Order collide directly with the Parties' First Amendment rights, including by seeking private IP address information and other details for all the Parties' Twitter messages posted over a period of more than six ½ months. The government

[8] The Parties recognize that the Fourth Circuit has wondered aloud in *dicta* about how the First Amendment may affect "the standards governing grand jury investigations." *In re Grand Jury 87-3 Subpoena*, 955 F.2d 229, 232-34 (4th Cir. 1992). But in that case, the real party's First Amendment rights were not implicated, so the Court avoided the substantial relationship test issue. *Id.* at 232-33. It specifically did not decide "the 'First Amendment versus Grand Jury' dilemma" that other courts have resolved by requiring the government to satisfy the substantial relationship test, as discussed above.

cannot claim that all—or even most—of these postings have anything to do with WikiLeaks, its criminal investigation, or matters to be considered by the grand jury. The Application and Order also seek details related to all direct messages between the Parties without any apparent showing that any such messages that might exist are related in any way to WikiLeaks, the government's criminal investigation, or matters to be considered by the grand jury. In light of these significant First Amendment concerns, the Government cannot use the Parties' purported association with WikiLeaks as a sufficient basis for obtaining the Twitter records here.

The Court should vacate its December 14 Order and reconsider in light of these First Amendment principles. Unless the government can show that the information sought would further a compelling interest and that the requests here are the least restrictive way to serve that interest, the government's efforts to seek private data regarding the Parties' Twitter use should be rejected.

C. The Order Should be Vacated Because it Threatens the Parties' Fourth Amendment Rights.

In addition to implicating the Parties' First Amendment rights, the Order threatens to violate Parties' Fourth Amendment rights as well. The Order threatens such rights because it requires the production of the IP addresses used by Parties at particular dates and times when they logged into their Twitter accounts. Such information could reveal when Parties were located in particular private spaces and is information in which the Parties maintain a constitutionally-protected reasonable expectation of privacy.

IP address information, linked to date and time, such as that sought in the December 14 Order, could allow the government to discern the physical location of the Parties at the exact time they were publishing on Twitter. As the Second Circuit explained:

> The Internet is comprised of numerous interconnected communications and computer networks connecting a wide range of end-users to each other. Every end-user's computer that is connected to the Internet is assigned a unique Internet Protocol number (IP address), such as 123.456.78.90, that identifies its location (*i.e.*, a particular computer-to-network connection) and serves as the routing address for email, pictures, requests to view a web page, and other data sent across the Internet from other end-users.

Register. com, Inc. v. Verio, Inc., 356 F. 3d 393, 409-410 (2nd Cir. 2004) (citation omitted). In

many instances, this information can then simply and easily be translated into the physical location of the speaker, based on publicly available information.[9] As one Court observed, "the process by which defendants IP addresses can be matched up with specific geographic designations, using a publicly available database operated by the American Registry for Internet Numbers. These geographic designations indicate the 'likely' locations of the residences or other venues where defendants used their Internet-connected computers." *Sony Music Entertainment Inc. v. Does 1-40*, 326 F. Supp. 2d 556, 567 (S.D.N.Y. 2004). To the extent that an IP address alone does not reveal physical location, an IP address in combination with the records of the Internal Service Provider that assigned the IP address to a particular subscriber can still reveal physical location, as explained in the Justice Department's computer search and surveillance manual:

> In a common computer search scenario, investigators learn of online criminal conduct. Using records obtained from a victim or from a service provider, investigators determine the Internet Protocol ("IP") address used to commit the crime. Using a subpoena or other process...investigators then compel the Internet Service Provider ("ISP") that has control over that IP address to identify which of its customers was assigned that IP address at the relevant time....

Computer Crime and Intellectual Property Section, Criminal Division, U.S. Department of Justice, Searching and Seizing Computers and Obtaining Evidence in Criminal Investigations, ch. II, § (C)(1)(a) at 65, available at http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.pdf (last visited Jan. 24, 2011). Thus, by demanding the IP addresses linked to each date and time that each of the Parties logged into the Twitter service over a multi-month period, the government can use such information to try to determine the Parties' locations at the very times they were engaged in publishing—regardless of whether the underlying speech was related to WikiLeaks, and regardless of whether they were Tweeting from a public or a private space.

The government's request for IP addresses here is significant given how such information

---

[9] The accuracy of IP Address geolocation can depend on many factors, including how an ISP has set up its network of servers and whether an Internet user utilizes one of several tools that allow Internet users to obfuscate their IP addresses. However, one of the leading companies advertises that its free gelolocation tool can determine the location of "79% [of U.S. IP addresses] within a 25 mile radius." MaxMind web site, <http://www.maxmind.com/app/geolitecity> (accessed November 19, 2010).

may reveal location information. Over a quarter of a century ago, the Supreme Court held in *United States v. Karo*, 468 US 705 (1984), that location tracking implicates Fourth Amendment privacy interests because it may reveal information about individuals in areas where they have reasonable expectations of privacy. In *Karo*, the police placed a primitive tracking device known as a beeper inside a can of ether and used it to infer that the ether remained inside a private residence. In considering the Fourth Amendment challenge to the use of the beeper, the Court held that using an electronic device to infer facts about "location[s] not open to visual surveillance," such as whether "a particular article is actually located at a particular time in the private residence," or to later confirm that the article remains on the premises, was just as unreasonable as searching the location without a warrant. *Karo*, 468 U.S. at 714-15. Such location tracking, the Court ruled, "falls within the ambit of the Fourth Amendment when it reveals information that could not have been obtained through visual surveillance" from a public place, whether it reveals that information directly or enables inferences about the contents of protected spaces. *Id.* at 707, *see also Kyllo v. United States*, 533 U.S. 27, 36 (2001) (rejecting "the novel proposition that inference insulates a search," noting that it was "blatantly contrary" to the Court's holding in *Karo* "where the police 'inferred' from the activation of a beeper that a certain can of ether was in the home."). This reasonable expectation of privacy in the contents of protected spaces is not limited to the home but extends to other private spaces as well.[10] *See, e.g., See v. City of Seattle*, 387 US 541, 543 (1967) (business premises); *Stoner v. California*, 376 U.S. 483 486 (1964) (hotel room).

---

[10] Although the Parties have not found any cases specifically addressing Twitter data, numerous courts have recognized that computer users also have a reasonable expectation of privacy in their computer-related data. *See Trulock v. Fresh*, 275 F.3d 391, 402-403 (4th Cir. 2001) (determining whether a search of computers was reasonable under 4th Amendment standards and holding that the plaintiff "had a reasonable expectation of privacy in the password protected computer files"); *United States v. Mann*, 592 F.3d 779, 786 (7th Cir. 2010) (reviewing computer searches under 4th Amendment standards and cautioning that those "involved in searches of digital media need to exercise caution to ensure that...searches are narrowly tailored to uncover on those things described" in a warrant); *United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999) (noting 4th Amendment concerns in searching computer stored data, particularly where relevant and non-relevant files are "intermingled" together); *see also United States v. Warshak*, 2010 WL 5071766 at ** 11, 14 (6th Cir. Dec. 14, 2010) (noting that given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment Protection" and therefore holding that "a subscriber enjoys a reasonable expectation of privacy in the contents of emails that are shared with, or sent or received through, a commercial ISP"").

Relying on *Karo* and *Kyllo*, the Third Circuit recently concluded that the records of a cell phone provider that indicate the location of a subscriber's cell phone ("cell site location information" or "CSLI") may violate the Fourth Amendment to the extent such records can establish that a cell phone was in a particular private space at a particular time. *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304 (3d Cir. 2010) ("*Third Circuit Opinion*"). Specifically, a majority of the Panel concluded that it "cannot reject the hypothesis that CSLI may, under certain circumstances, be used to approximate the past location of a person. If it can be used to allow the inference of present, or even future, location, in this respect CSLI may resemble a tracking device which provides information as to the actual whereabouts of the subject" and is therefore protected under *Karo*. *Third Circuit Opinion*, 620 F.3d at 312; *see also id.* at 320 (Tashima, J., concurring) (citing *Kyllo* for the proposition that government access to CSLI absent a showing of probable cause would violate the Fourth Amendment if that information "reveals a cell phone user's location within the interior or curtilage of his home").

Importantly, the Third Circuit held that a cell phone user's Fourth Amendment interest in CSLI is not eliminated by the fact that such information is a record of the phone company. Distinguishing the telephone dialing information that the Supreme Court found to be unprotected under the Fourth Amendment in *Smith v. Maryland*, 442 U.S. 735, 744-45 (1979), the Court emphasized that cell phone users do not voluntarily convey their location to the phone company. When a cell phone user makes a call, the only information voluntarily and knowingly conveyed to the phone company is the number that is dialed—there is no indication to the user that making that call will also locate the caller, let alone generate a permanent record of this location. When a cell phone user receives a call, he has not voluntarily exposed anything at all. *See Third Circuit Opinion*, 620 F.3d at 317 (It is "unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information[,]" therefore "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way.").

The same logic applies to the Parties' records here. Even though records are held by

Twitter, like with CSLI, Twitter users do not voluntarily convey their IP address to the Twitter internet site they visit in a manner that is analogous to the dialing of a telephone. Similarly, as with CSLI, it is unlikely that typical Internet users have any awareness of their IP address, or the fact that it is transmitted to the Internet sites that they communicate with such as Twitter.

The conclusion that IP address information is protected by the Fourth Amendment is further bolstered by the D.C. Circuit's recent conclusion that warrantless use of a GPS device to track the movements of an individual's car over the course of a month violates Fourth Amendment protections. *United States v. Maynard*, 615 F.3d 544, 559 (D.C. Cir. 2010), *pet. for reh'g en banc denied* (D.C. Cir. Nov. 19, 2010). As that court explained, even though the car might move in public spaces, "the whole of one's movements over the course of a month is not constructively exposed to the public" and "prolonged GPS monitoring" reveals an intimate picture of the subject's life that he expects no one to have." *Id.* at 561-63. Similarly here, IP address information can reveal an intimate portrait of Parties' movements between the private spaces from which they use the Twitter service.

Thus, the Court, therefore should vacate its December 14 Order and reconsider the government's Application in light of the principles set forth in *Karo*, the *Third Circuit Opinion* and *Maynard*.

D. The Court Should Exercise its Discretion Under 18 U.S.C. § 2703(d) and Avoid Serious Constitutional Questions by Vacating the Order and Requiring a Warrant.

In light of the serious constitutional questions that the Order raises under both the First and Fourth Amendments, if the Court does not vacate the Order completely it should exercise its discretion under § 2703(d) and avoid these constitutional questions by requiring the Government to obtain a warrant based on probable cause.

Although the Stored Communications Act ("SCA") allows the Government to obtain the records sought from Twitter through a court order issued under 18 U.S.C. § 2703(d), the statute also provides courts with the discretion to deny applications for such orders even when the government has made the factual showing required under that section. *Third Circuit Opinion*, 620 4.3d at 315-17. The statute does so by its use of the phrase "only if" in § 2703(d), indicating that the "specific and articulable facts" showing required by that section is a necessary but not

necessarily sufficient condition for a § 2703(d) order. *Id.* The practical effect of such a denial is that the government must instead proceed by obtaining a search warrant based on probable cause, issued under Rule 41 of the Federal Rules of Criminal Procedure pursuant to 18 U.S.C. § 2703(c)(1)(a). *See id.* at 316. Therefore, "the statute as presently written gives the [judge] the option to require a warrant showing probable cause...." *Id.* at 319.[11]

The intent of this "sliding scale" construction of § 2703 is evidenced by Congress' recognition that the Constitution may in some cases protect the privacy of information that would otherwise be available to the Government under § 2703(d). As the Senate Judiciary Committee's report on the statute explained:

> With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal and business information. . . . For the person or business whose records are involved, the privacy or proprietary interest in that information should not change. Nevertheless, because it is subject to control by a third party computer operator, the information *may* be subject to no constitutional privacy protection.

S. Rep. No. 99-541 at 3 (1986) (emphasis added); *see also, e.g.*, S. Hrg. 98-1266 at 17 (1984) ("In this rapidly developing area of communications which range from cellular non-wire telephone connections to microwave-fed computer terminals, distinctions such as [whether a participant to an electronic communication can claim a reasonable expectation of privacy] are *not always clear or obvious*.") (emphasis added). In the context of such constitutional uncertainty, it makes sense that Congress would provide a constitutional safety-valve for judges considering government applications under § 2703(d), thereby future-proofing the statute by

---

[11] Ms. Jonsdottir's counsel, EFF and ACLU, served as *amici* to the Third Circuit and the Western District of Pennsylvania on this issue and their briefs provide extensive support for the *Third Circuit Opinion*'s holdings. *See* Brief for Electronic Frontier Foundation, American Civil Liberties Union, ACLU Foundation of Pennsylvania, and Center for Democracy and Technology as Amici Curiae Opposing the Government's Request for Review, *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, Magistrate's No. 07-524M, 2008 WL 4191511 (W.D. Pa. 2008), *available at* https://www.eff.org/files/filenode/celltracking/LenihanAmicus.pdf; Brief for Electronic Frontier Foundation et al. as Amici Curiae Supporting Affirmance, *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304 (3d Cir. 2010), *available at* https://www.eff.org/files/filenode/celltracking/Filed%20Cell%20Tracking%20Brief.pdf; Brief for Electronic Frontier Foundation et al. as Amici Curiae Opposing Rehearing En Banc, *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304 (3d Cir. 2010), *available at* https://www.eff.org/files/Filed_Amicus_Opp_to_En_Banc_Petition.pdf

allowing courts the discretion to deny such applications to avoid potential constitutional violations or unnecessary constitutional rulings.

Considering the longstanding doctrine of constitutional avoidance, and particularly in light of the Supreme Court's recent admonition that courts should avoid unnecessary rulings on how the Fourth Amendment applies to new technologies, a Court would properly use its discretion under § 2703(d) when faced with a government application that raises serious constitutional questions. *See City of Ontario v. Quon*, 130 S. Ct. 2619, 2629, 177 L. Ed. 2d 216 (2010) ("The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."); *Ashwander v. Tennessee Valley Auth.*, 297 U.S. 288, 347-48 (1936) ("The Court will not pass upon a constitutional question although properly presented by the record, if there is also present some other ground upon which the case may be disposed of.").

As detailed above, the government's Application presents these sort of serious questions—raising serious First and Fourth Amendment concerns. The Court, therefore, should exercise its discretion under § 2703(d), vacate the Dec. 14 Order, and require the government instead to obtain a warrant based on probable cause.

E. The Request for Information about a Member of the Icelandic Parliament, Ms. Jonsdottir, Raises Additional Concerns.

The government's demand for records for Ms. Jonsdottir, an elected member of the Icelandic Parliament, raises additional concerns. Such an investigation appears to violate Icelandic law. As indicated by the attached letter from the Acting Permanent Secretary of State for Iceland, Sears Decl, Exh. 5, and the Decision by the Inter-Parliamentary Union, Sears Decl., Exh. 6, Ms. Jonsdottir is protected by a strong constitutional immunity in Iceland, rooted in Article 49 of the Icelandic Constitution and a similar provision in the Icelandic Law on criminal procedure. Similar immunities exist for Parliamentarians around the world.[12] Ms. Jonsdottir's Tweets are predominantly in Icelandic and largely concern issues arising in Iceland, such as legislation sponsored by Ms. Jonsdottir, the Icelandic debt crisis, and the Icelandic volcanic

[12] The members of the U.S. Congress enjoy similar immunities, rooted in Article I, Section 6, Clause 1, of the U.S. Constitution.

eruption. *See* Sears Decl., Exh. 4. Thus, the government's overbroad demand for information about Ms. Jonsdottir creates a situation where the U.S. government is conducting a criminal investigation which sweeps in Ms. Jonsdottir's publications in Icelandic on topics of Icelandic concern—records that could not be obtained under Icelandic law.

Unfortunately this investigation creates a perilous precedent for foreign government efforts to seek information about members of the U.S. Congress. This concern is yet another reason why the Order should be vacated as to Ms. Jonsdottir.

IV. CONCLUSION

For the foregoing reasons the Court should vacate its December 14, 2010 Order requiring Twitter to disclose the Parties' Twitter records related to the Parties and their accounts associated with "rop_g"; "ioerror", and "birgittaj."

Dated: January 26, 2011

By: _____

John K. Zwerling, VSB No. 8201
Stuart Sears, VSB No. 71436
ZWERLING, LEIBIG & MOSELEY, P.C.
108 North Alfred Street
Alexandria, VA 22314
Telephone: (703) 684-8000
Facsimile: (703) 684-9700
Email: JZ@Zwerling.com
Email: Chris@Zwerling.com
Email: Andrea@Zwerling.com
Email: Stuart@Zwerling.com

John W. Keker (*pro hac vice* pending)
Rachael E. Meny (*pro hac vice* pending)
Steven P. Ragland (*pro hac vice* pending)
KEKER & VAN NEST LLP
710 Sansome Street
San Francisco, CA 94111-1704
Telephone: (415) 391-5400
Facsimile: (415) 397-7188
Email: jkeker@kvn.com
Email: rmeny@kvn.com
Email: sragland@kvn.com

Attorneys for JACOB APPELBAUM

Dated: January 26, 2011

By: /s/ with permission for

Nina J. Ginsberg, VSB No. 19472
DIMUROGINSBERG, P.C.
908 King Street, Suite 200
Alexandria, VA 22314
Phone: 703-684-4333
Fax: 703-548-3181
Email: nginsberg@dimuro.com

John D. Cline (*pro hac vice* pending)
LAW OFFICE OF JOHN D. CLINE
115 Sansome Street, Suite 1204
San Francisco, CA 94104
Phone: 415.322.8319
Fax: 415.524.8265
Email: cline@johndclinelaw.com

K.C. Maxwell (*pro hac vice* pending)
LAW OFFICE OF K.C. MAXWELL
115 Sansome Street, Suite 1204
San Francisco, CA 94104
Phone: 415.322.8817
Fax: 415.888.2372
Email: kcm@kcmaxlaw.com

Attorneys for ROP GONGGRIJP

Dated: January 26, 2011

By: _____ with permission for:

Rebecca K. Glenberg, VSB No. 44099
AMERICAN CIVIL LIBERTIES UNION
OF VIRGINIA FOUNDATION, INC.
530 E. Main Street, Suite 310
Richmond, Virginia 23219
Telephone: (804) 644-8080
Facsimile: (804) 649-2733
Email: rglenberg@acluva.org

Cindy A. Cohn (*pro hac vice* pending)
Lee Tien (*pro hac vice* pending)
Kevin S. Bankston (*pro hac vice* pending)
Marcia Hofmann (*pro hac vice* pending)
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x108
Facsimile: (415) 436-9993
Email: cindy@eff.org
Email: tien@eff.org
Email: bankston@eff.org
Email: marcia@eff.org

Aden J. Fine (*pro hac vice* pending)
Benjamin Siracusa-Hillman (*pro hac vice* pending)
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Telephone: (212) 549-2500
Facsimile: (212) 549-2651
Email: afine@aclu.org
Email: bsiracusahillman@aclu.org

Attorneys for BIRGITTA JONSDOTTIR

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing pleading was delivered by hand this 26th day of January, 2011, to the U.S. Attorney Box located in the Clerk's office, addressed to:

[redacted]
U.S. Attorney's Office
2100 Jamieson Avenue
Alexandria, VA 22314
[redacted]

Stuart Alexander Sears

EXHIBIT 4

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

IN RE 2703(d) ORDER AND 2703(f) PRESERVATION REQUEST RELATING TO GMAIL ACCOUT [redacted]	)	Misc. No. 10GJ3793 FILED UNDER SEAL

ORDER

FOR REASONS stated from the bench and in accord with specific rulings and instructions thereto, it is hereby

ORDERED that Google's Motion to Modify 2703(d) Order for Purpose of Providing Notice to User is **DENIED in part and GRANTED in part**; the motion is **DENIED** as to Google's request to notify the user concerning the 2703(d) Order and the underlying application; the motion is **GRANTED** in regard to the request to modify the Order. In that regard, it is further

ORDERED that Google is authorized to provide notification of this Court's 2703(d) Order, dated January 4, 2011, to the Google Gmail user [redacted] within (90) days of providing to the United States government the information requested in said Order, unless the government files a motion for an extension of that non-notification period; it is further

ORDERED that the government may request an extension of the non-notification period for a maximum of sixty (60) days.

A TRUE COPY, TESTE:
CLERK, U.S. DISTRICT COURT

BY [redacted]
DEPUTY CLERK

The Clerk is directed to file this Order under Seal and to forward copies of this Order to all counsel of record.

ENTERED this 9th day of February 2011.

United States Magistrate Judge

Alexandria, Virginia

EXHIBIT 5

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE §2703(d) ORDER RELATING TO TWITTER ACCOUNTS: [redacted]	)	MISC. NO. 10GJ3793

ORDER TO UNSEAL THE ORDER PURSUANT TO 18 U.S.C. §2703(D)

This matter having come before the Court pursuant to an application under Title 18, United States Code, §2703(d), it appearing that it is in the best interest of the investigation to unseal the Court's Order of December 14, 2010 and authorize Twitter to disclose that Order to its subscribers and customers, it is hereby ORDERED that the above-captioned Order of December 14, 2010 pursuant to 18 U.S.C. §2703(d) be UNSEALED and that Twitter is authorized to disclose such Order. In all other respects, the Court's Order of December 14, 2010 remains in effect.

[redacted]

THE HONORABLE [redacted]
UNITED STATES MAGISTRATE JUDGE

Date: 1/5/11

Alexandria, Virginia

EXHIBIT 6

FAX TRANSMISSION

United States Attorney
Eastern District of Virginia
Justin W. Williams U.S. Attorney's Office Building
2100 Jamieson Ave.
Alexandria, VA 22314

To	Custodian of Records Google
Fax	650-849-2939; 650-249-3429
From	[redacted] **Voice** 703-299-3700 Assistant United States Attorney
Fax	[redacted]
Date	January 12, 2011 **Pages** 3, including this page
Subject	Preservation letter under 18 U.S.C. sec. 2703(f)

U.S. Department of Justice

United States Attorney
Eastern District of Virginia

Justin W. Williams U.S. Attorney's Office Building
2100 Jamieson Ave.
Alexandria, VA 22314
PHONE: 703-299-3712

January 12, 2011

Google
1600 Amphitheatre Parkway
Mountain View, CA 94043

Attn: Custodian of Records
Facsimile: 650-649-2939; 650-249-3429

Re: Request for Preservation of Records

Dear Google:

Pursuant to Title 18, United States Code, Section 2703(f), this letter is a formal request for the preservation of all stored communications, records, and other evidence in your possession regarding the following email account pending further legal process: [redacted] the Account") November 2009 to the present.

I request that you not disclose the existence of this request to the subscriber or any other person, other than as necessary to comply with this request. If compliance with this request might result in a permanent or temporary termination of service to the Account, or otherwise alert any user of the Account as to your actions to preserve the information described below, please contact me as soon as possible and before taking action.

I request that you preserve, for a period of 90 days, the information described below currently in your possession in a form that includes the complete record. This request applies only retrospectively. It does not in any way obligate you to capture and preserve new information that arises after the date of this request. This request applies to the following items, whether in electronic or other form, including information stored on backup media, if available:

1. The contents of any communication or file stored by or for the Account and any associated accounts, and any information associated with those communications or files, such as the source and destination email addresses or IP addresses.

2. All records and other information relating to the Account and any associated accounts including the following:

   a. subscriber names, user names, screen names, or other identities;

b. mailing addresses, residential addresses, business addresses, e-mail addresses, and other contact information;

c. length of service (including start date) and types of service utilized;

d. records of user activity for any connections made to or from the Account, including the date, time, length, and method of connections, data transfer volume, user name, and source and destination Internet Protocol address(es);

e. telephone records, including local and long distance telephone connection records, caller identification records, cellular site and sector information, GPS data, and cellular network identifying information (such as the IMSI, MSISDN, IMEI, MEID, or ESN);

f. telephone or instrument number or other subscriber number or identity, including temporarily assigned network address;

g. means and source of payment for the Account (including any credit card or bank account numbers) and billing records;

h. correspondence and other records of contact by any person or entity about the Account, such as "Help Desk" notes; and

i. any other records or evidence relating to the Account.

If you have questions regarding this request, please call me at [redacted]

Sincerely,

[redacted]
UNITED STATES ATTORNEY

[redacted]
Assistant United States Attorney

EXHIBIT 7

THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE 2703(d) ORDER AND 2703(f) PRESERVATION REQUEST RELATING TO GMAIL ACCOUNT	Case No. 1:10GJ3793 11-DM-2 UNDER SEAL

RESPONSE OF THE UNITED STATES TO GOOGLE'S MOTION TO MODIFY 2703(d) ORDER FOR PURPOSE OF PROVIDING NOTICE TO USER

In its January 18, 2011 motion and supporting memorandum, Google Inc. ("Google") asks this Court to amend its January 4, 2011 order (the "Order") to allow Google to provide immediate notice of the Order to the subscriber of the [redacted]gmail.com account (the "[redacted] subscriber"), whose records are the subject of the Order. Google also asks that the Order be unsealed; requests permission to discuss the Order with the [redacted]ubscriber and his attorneys; and further requests that the [redacted] subscriber be given 20 days from the date of the Court's order to file an appropriate response. For the reasons set forth below, the United States opposes Google's motion and requests that the Court's current order of notice preclusion be maintained and that the Court not permit Google to provide the [redacted]ubscriber with immediate notice of the Order. However, as the United States explained to Google on January 12, 2011, the United States does not oppose a modification to the Order that would limit the non-disclosure period to 90 days, with a provision that would allow the government to petition the Court for an additional extension of this period consistent with the requirements of 18 U.S.C. § 2705(b).

[redacted]

ATTACHMENT H

THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE 2703(d) ORDER AND 2703(f) PRESERVATION REQUEST RELATING TO GMAIL ACCOUNT	Case No. 1:10GJ3793 11-DM-2 **UNDER SEAL**

RESPONSE OF THE UNITED STATES TO GOOGLE'S OBJECTIONS TO MAGISTRATE'S ORDER OF FEBRUARY 9, 2011

The United States, by and through [redacted], United States Attorney, opposes Google Inc.'s ("Google") objections to Magistrate Judge [redacted] decisions that the court-ordered legal process for business records pursuant to the Stored Communications Act ("SCA") (18 U.S.C. §§ 2701-12) should remain under seal and not be disclosed for a limited period of time pending the ongoing criminal investigation.

Specifically, in its pleading, Google objects[1] to Magistrate [redacted] ruling on February 9, 2011 that denied in part and granted in part Google's motion to modify the court's order of January 4, 2011 (the "Order") requiring Google to produce subscriber and transaction records related to the Gmail account [redacted] (whose subscriber will be referred to as the [redacted] subscriber") under 18 U.S.C. § 2703(d). Google had asked Judge [redacted] to unseal and vacate the Order's non-disclosure provisions, which the court properly included pursuant to 18 U.S.C. § 2705 and Local Criminal Rule 49, so that Google could "provide *immediate* notice" to

[1] Google styles its pleading as "objections" and "notice of appeal." Google's objections have been made pursuant to Fed.R.Crim. P. 59. *See* Google Mot. at 8. Google has no procedural basis to appeal, however, and to the extent Google has sought an appeal, the government requests that the Court either dismiss it or treat it as an objection. *Compare* 18 U.S.C. § 3402 and Fed.R.Crim.P. 58(g).

the [redacted] subscriber. Google Mot. at 2 (emphasis added). Magistrate [redacted] adopted, instead, the government's reasonable proposal to modify the Order to authorize Google to provide notice to the [redacted] subscriber "within (90) days of providing . . . the information requested in [the] Order, unless the government files a motion for an extension of that non-notification period." Roche Decl. Ex. 4. Magistrate [redacted] further ordered "that the government may request an extension of the [Order's] non-notification period for a maximum of sixty (60) days." ("Order 2") *Id.*

For the reasons set forth below, the United States opposes Google's objections and requests that the Court find that the two Orders are proper under the SCA, Local Criminal Rule 49, and the Constitution, and that Judge [redacted] committed no error, let alone any clear error.

Factual & Procedural Background

On January 4, 2011, upon application of the United States pursuant to § 2703(d), finding that the information sought was relevant and material to an ongoing criminal investigation, Judge [redacted] issued the Order, requiring Google to produce the following non-content business subscriber and transaction records for the ioerror subscriber's account:

A. The following customer or subscriber account information for each account registered to or associated with [redacted] for the time period November 1, 2009 to the present:

1. subscriber names, user names, screen names, or other identities;
2. mailing addresses, residential addresses, business addresses, e-mail addresses, and other contact information;
3. connection records, or records of session times and durations;
4. length of service (including start date) and types of service utilized;
5. telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

6. means and source of payment for such service (including any credit card or bank account number) and billing records.

B. All records and other information relating to the account(s) and time period in Part A, including:

1. records of user activity for any connections made to or from the Account, including the date, time, length, and method of connections, data transfer volume, user name, and source and destination Internet Protocol address(es);

2. non-content information associated with the contents of any communication or file stored by or for the account(s), such as the source and destination email addresses and IP addresses.

3. correspondence and notes of records related to the account(s).

See Roche Decl. Ex. 1. The contents of the [redacted]ubscriber's communications were not required. After finding "that prior notice of this Order to any person of this investigation or this application and Order entered in connection therewith would seriously jeopardize the investigation," Judge [redacted]rdered that "the application and this Order are sealed until otherwise ordered by the Court, and that Google shall not disclose the existence of the application or this Order of the Court, or the existence of the investigation, to the listed subscriber or to any other person, unless and until authorized to do so by the Court." *Id.*

Several weeks earlier, on December 14, 2010, Magistrate Judge [redacted] had issued a different order, also pursuant to 18 U.S.C. § 2703(d), that required Twitter, Inc. ("Twitter") to disclose similar categories of non-content business records for several Twitter accounts, including a Twitter account under the name [redacted] *See* Roche Decl. Ex. 2. This order (the "Twitter Order"), like the Order, was issued under seal and contained a non-disclosure provision that prohibited Twitter from disclosing the existence of the application, the Twitter Order, or the existence of the investigation to any person, unless and until authorized to do so by the Court. *See id.* After learning that Twitter would file a motion to modify the Twitter Order

so it could disclose it to its customers and subscribers, the government replied that although it was not conceding the merits, it would voluntarily agree to move to unseal the Twitter Order to allow such disclosure.

On January 5, 2011, Magistrate Judge [redacted] granted the government's application to unseal the Twitter Order and authorized Twitter to disclose it ("Twitter Unsealing Order") based on the government's representation that it was in the best interest of the investigation to permit disclosure to Twitter's subscribers and customers. *See* Roche Decl. Ex. 5. The government sent the Twitter Unsealing Order to counsel for Twitter on January 7, 2011.

On January 12, 2011, counsel for Google asked the government to agree to modify the Order to allow Google to provide immediate notice of the Order to the [redacted] subscriber. *See* Google Mot. at 7. The government did not agree to this proposed modification. When asked why the government was taking a different position on Google's request to modify the Order than it had taken on Twitter's similar request, the government responded, "It's a different case." This response was intended as a general comment of the different circumstances surrounding the two Orders and was not intended to be an assertion that the Orders related to different investigations. Roche Decl. Ex. 7 at 3, n. 1. The government, did however, offer to agree to a 90-day limit on the non-disclosure period, subject to a provision that would allow the government to petition for extensions if disclosure would seriously jeopardize the investigation or have an adverse result listed in 18 U.S.C. § 2705. Google declined this offer and filed its motion to modify the Order on January 18, 2011. Google Mot. at 7. On February 9, 2011, following a hearing, Magistrate Judge [redacted] enied Google's motion in part, as described in more detail above. Google now objects to this order.

Argument

I. Standard of Review

Google filed its objections pursuant to Federal Rule of Criminal Procedure 59, and therefore this Court should review Google's objections in accordance with the procedures of that rule.[2] *See* Google Mot. at 8. Rule 59(a) authorizes a party to file objections to a magistrate judge order that determines "any matter that does not dispose of a charge or defense," Fed. R. Crim. P. 59(a), while Rule 59(b) authorizes a party to file objections to a magistrate judge's "proposed findings and recommendations" for disposing of "a defendant's motion to dismiss or quash an indictment or information, a motion to suppress evidence, or any matter that may dispose of a charge or defense." Fed. R. Crim. P. 59(b)(1), (2). In the instant matter, Judge [redacted] denial of Google's motion is an order that "does not dispose of any charge or defense," Fed. R. Crim. P. 59(a), and therefore Google's objections to this ruling fall within the ambit of Rule 59(a). Indeed, at least two district courts have reviewed magistrate decisions about § 2703(d) orders under Rule 59(a). *See In re U.S. for Order Directing a Provider of Electronic*

---

[2] The objection procedures in Rule 59 apply when a district judge has referred to a magistrate judge any matter or motion that falls within the scope of subparts (a) and (b). *See* Fed. R. Crim. P. 59(a), (b). Although there was no individual referral in this case, the district judges in this district have "authorized and specially designated" magistrate judges "to perform all duties authorized or allowed to be performed by United States magistrate judges by the United States Code and any rule governing proceedings in this court." E.D. Va. Local Cr. Rule 5. Pursuant to this Local Rule, Judge [redacted] was authorized to issue the § 2703(d) order to Google because such orders "may be issued by any court that is a court of competent jurisdiction," 18 U.S.C. § 2703(d), which includes a magistrate judge of any district court of the United States that has jurisdiction over the offense being investigated. *See* 18 U.S.C. § 2711(3)(A) (defining "court of competent jurisdiction"); 28 U.S.C. § 636(b)(3) ("A magistrate judge may be assigned such additional duties as are not inconsistent with the Constitution and laws of the United States."). Accordingly, the government agrees that Google may file its objections to Judge Davis's Order pursuant to Rule 59.

Communication Service to Disclose Records to the Government, 2008 WL 4191511, at *1 (W.D. Pa. 2008), *vacated on other grounds by* 620 F.3d 304 (3d Cir. 2010) (reviewing objections to magistrate judge's denial of a § 2703(d) court order under Fed. R. Crim. P. 59(a) and 28 U.S.C. § 636(b)(1)); *In re U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Information*, 2006 WL 2871743, at *1 (E.D. Wisc. 2006) (same).

Under Rule 59(a), this Court must determine whether Judge [redacted] ruling was "contrary to law or clearly erroneous" and should not modify or set aside his order unless this standard is met. Fed. R. Crim. P. 59(a); *see also* 28 U.S.C. § 636(b)(1)(A) ("A judge of the court may reconsider any pretrial matter under this subparagraph (A) where it has been shown that the magistrate judge's order is clearly erroneous or contrary to law."); *GTSI Corp. v. Wildflower Int'l, Inc.*, 2009 WL 3245396, at *2 (E.D. Va. 2009) (district court should overturn magistrate judge's civil non-dispositive discovery order only if it is "clearly erroneous or contrary to law"). In addition, because Judge [redacted] was the judicial officer who issued the § 2703(d) order, his "decision to seal, or to grant access, is subject to review under an abuse of discretion standard." *Baltimore Sun Co. v. Goetz*, 886 F.2d 60, 65 (4th Cir. 1989) ("[T]he common law qualified right of access to the warrant papers is committed to the sound discretion of the judicial officer who issued the warrant."); *see Media General Operations, Inc. v. Buchanan*, 417 F.3d 424, 429 (4th Cir. 2005) (quoting *Goetz*).

The parties disagree on the appropriate standard of review. Google suggests that Judge [redacted] order should be considered "dispositive," thereby requiring this Court to review Google's objections under the *de novo* standard set forth in Rule 59(b). *See* Google Mot. at 9. But, Rule 59(b) is inapplicable here. Pursuant to his authority under Local Criminal Rule 5 and 18 U.S.C. § 2703(d), Judge [redacted] issued an order, not "proposed findings and recommendations"

that would be subject to review under Rule 59(b). Furthermore, Google's original motion is nondispositive for purposes of Rule 59 because it "does not dispose of a charge or defense," Fed. R. Crim. 59(a), and it is not a motion to dismiss or quash an indictment or information or a motion to suppress evidence. Fed. R. Crim. P. 59(b)(1); *cf. Aluminum Co. of Am., Badin Works, Badin, N.C. v. U.S. Envtl. Prot. Agency*, 663 F.2d 499, 501 (4th Cir. 1981) (motion to quash ex parte administrative search warrant was dispositive for purposes of 28 U.S.C. § 636(b) when it "was not a 'pretrial matter' but set forth all of the relief requested"); *compare In re Oral Testimony of a Witness Subpoenaed*, 182 F.R.D. 196, 200-202 (E.D. Va. 1998) (for purposes of determining if a magistrate order is dispositive, distinguishing administrative subpoenas, which are final, appealable orders, from orders enforcing subpoenas issued in connection with civil and criminal actions, or with grand jury proceedings, which are normally not considered final) (citing *Reich v. National Engineering & Contracting Co.*, 13 F.3d 93, 95 (4th Cir.1993) (other citations omitted).

Google's motion simply sought to modify a § 2703(d) order that was issued as part of a pending grand jury investigation. It, therefore, falls within Rule 59(a), not Rule 59(b). The cases Google cites in support of *de novo* review are inapposite as they apply to whether a district court order is "immediately appealable final order" for purposes of appellate review under 28 U.S.C. § 1291, not to whether a Magistrate's Order is dispositive or non-dispositive under Rule 59.[3] Thus, the standard for this Court's review is whether Judge [redacted] ruling was "contrary to law or clearly erroneous." Fed. R. Crim. P. 59(a).

---

[3] Even assuming that Judge [redacted]'s denial of Google's motion is an "immediately appealable final order" for purposes of establishing appellate jurisdiction under 28 U.S.C. § 1291, Google Mot. at 9 (quoting *United States v. Myers*, 593 F.3d 388, 345 (4th Cir. 2010)), it does not follow that Judge [redacted] order was "dispositive" for purposes of Rule 59(b). *Cf. United States v. Raddatz*, 447 U.S. 667, 673 (1980) (observing that "the magistrate has no authority to make a

II. The Orders Are Proper

Magistrate Judge [redacted] two Orders satisfy all statutory and constitutional requirements, and the sealing and non-disclosure provisions should remain in effect for the limited time provided in Order 2. Judge [redacted] committed no error in issuing the Orders and certainly committed no clear error. Google has no statutory basis to challenge the sealing and non-disclosure provisions of the Orders, and the [redacted] subscriber would not have a valid basis to challenge the Order even if Google did provide him with notice. In addition, unsealing and permitting disclosure at this time is not in the best interest of the investigation. The unsealing and disclosure of the Twitter Order has already seriously jeopardized the investigation, and the government believes that further disclosures at this time will exacerbate the harm caused by that disclosure.

A. The Non-Disclosure and Sealing Provisions of the Order Are Proper Under 18 U.S.C. § 2705(b) and Local Criminal Rule 49.

As Judge [redacted] concluded, the non-disclosure provision of the Order is appropriate under 18 U.S.C. § 2705(b). Under § 2705(b), the government may apply for an order commanding a provider, such as Google, not to notify any other person of the existence of the order for such period as the court deems appropriate. *See* 18 U.S.C. § 2705(b). The court, in turn, shall issue the requested order:

> if it determines that there is reason to believe that notification of the existence of the . . . court order will result in—
>
> (1) endangering the life or physical safety of an individual;
>
> (2) flight from prosecution;

---

final and binding disposition" as to a "dispositive" motion covered by 28 U.S.C. § 636(b)(1)(B)). In fact, a "final order" of a magistrate judge would fall more squarely within the scope of Rule 59(a), which applies when a magistrate judge has entered "an oral or written order stating the [magistrate judge's] determination." Fed. R. Crim. P. 59(a).

(3) destruction of or tampering with evidence;

(4) intimidation of potential witnesses; or

(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

18 U.S.C. § 2705(b).

Judge [redacted] also appropriately sealed the Order. It is generally recognized that the public has a common law right of access, but not a First Amendment right of access, to judicial documents, including documents associated with *ex parte* proceedings such as search warrant affidavits. *Media General Operations, Inc. v. Buchanan*, 417 F.3d 424, 429 (4th Cir. 2005); *In re Washington Post Company v. Hughes*, 923 F.2d 324, 326 (4th Cir. 1991). "But the right of access is qualified, and a judicial officer may deny access to search warrant documents if sealing is 'essential to preserve higher values' and 'narrowly tailored to serve that interest.'"[4] *Media General Operations*, 417 F.3d at 429 (citations omitted); *see also In re Knight Pub. Co.*, 743 F.2d 231, 235 (4th Cir. 1984) ("[t]he trial court has supervisory power over its own records and may, in its discretion, seal documents if the public's right of access is outweighed by competing interests"). Sealing search warrants and their accompanying affidavits and applications is within

[4] One such "higher value" is the protection of an ongoing criminal investigation. Process that is issued in connection with an investigation into criminal activity serves "a compelling state interest." *In re Grand Jury Subpoena: Subpoena Duces Tecum*, 829 F.2d 1291, 1305 (4th Cir. 1987) (Wilkinson, J., concurring) (citing *Branzburg v. Hayes*, 408 U.S. 665, 700 (1972)). This is true no matter what criminal conduct is under investigation, as the compelling state interest "does not turn" on the type of crime involved. *Id.* The secrecy of criminal investigations is an essential tool to further that interest. "[L]aw enforcement agencies must be able to investigate crime without the details of the investigation being released to the public in a manner that compromises the investigation." *Va. Dept. of State Police v. Washington Post*, 386 F.3d 567, 574 (4th Cir. 2004); *see also Times Mirror Co. v. United States*, 873 F.2d 1210, 1215 (9th Cir. 1989) ("In other words, the secrecy of grand jury proceedings is maintained in large part to avoid jeopardizing the criminal investigation of which the grand jury is an integral part.").

the discretionary powers of a judicial officer where, among other things, an "'affidavit contain[s] sensitive details of an ongoing investigation' and it is 'clear and apparent from the affidavits that any disclosure of the information there would hamper' th[e] ongoing investigation." *Media General Operations,* 417 F.3d at 430 (citations omitted); *see also In re Search Warrant for Matter of Eye Care Physicians of America,* 100 F.3d 514, 518 (7th Cir. 1996).

The government's application, without more, provided sufficient basis for Judge Davis to conclude that notifying the [redacted] subscriber of the Order will have one or more of the adverse results listed in § 2705(b). *See* Government Exhibit 1 *(ex parte)*. Based on this information, Judge [redacted] appropriately decided to maintain the Order under seal and prohibit its disclosure.

The adverse results of disclosing and unsealing the Twitter Order, including efforts to conceal evidence and harassment (discussed in Part III), further confirm that unsealing and disclosing the Order would seriously jeopardize the investigation. Therefore, this Court should find that the non-disclosure and sealing provisions in the Order are proper under 18 U.S.C. § 2705(b) and L. Crim. R. 49. Judge [redacted] committed no error by including such provisions in the Order, let alone clear error.

B. Google Has No Statutory Basis to Challenge the Non-Disclosure and Sealing Provisions in the Order.

Judge [redacted] correctly concluded that Google has no statutory basis to challenge the non-disclosure and sealing provisions in the Order. Pursuant to § 2703(d), a service provider, such as Google, may move to quash or modify an 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). However, as described in more detail below, Google has not shown – and cannot show – that complying with the non-disclosure provisions of the Order would cause an "undue burden" on Google.

At the hearing on February 9, 2011, when asked about its statutory authority to bring a motion to modify the Order, Google could cite only to § 2703(d).[5] First, Google claimed that it would be an undue burden for it to comply with an Order it believed may be unlawful: Google did not believe that the government could make the showing required for sealing and non-disclosure when the government had agreed to unseal the Twitter Order one day before it obtained the Order in this case. Judge [redacted] explained that § 2703(d) contained no provision allowing a provider or subscriber to move to quash or modify an Order that the provider believed to be improperly issued. Further, Judge [redacted] reasoned that Google had no evidence that the Order was improperly issued. Finally, Google could not show that compliance would cause an undue burden as required to quash or modify the Order under § 2703(d). *See* 18 U.S.C. § 2703(d). This is because under § 2703(e), no customer could successfully sue Google for complying with the Order because the SCA prohibits causes of action against providers for providing information in accordance with the terms of a court order. *See* 18 U.S.C. § 2703(e).

Second, Google argued that the Order was unlawful, and therefore, imposed an undue burden because the perpetual nature of its non-disclosure provision. Google conceded that this undue burden argument would be weakened, however, if Judge [redacted] modified the Order to include a 90-day limit on the non-disclosure period. Third, Google argued that the Order imposed an undue burden because it affected Google's goodwill with customers, who might be prejudiced by Google's compliance with the Order. *See generally,* Google Mot. at 3.[6] Judge

---

[5] The information in this paragraph is based on notes from the hearing and is not a verbatim transcript of the events. Google was unable to point to any other provision for good reason, § 2708(d) provides that "[t]he remedies and sanctions described in" the SCA are the "only judicial remedies and sanctions for nonconstitutional violations of [the SCA]." 18 U.S.C. § 2708; *United States v. Clenney,* --- F.3d ---, 2011 WL 322640 at * 8 (4th Cir. 2011).

[6] Google has failed to support this assertion, however, by pointing to a relevant privacy policy statement or by citing to any other occasion when it challenged a non-disclosure provision in a §

[redacted] found, however, that even assuming an undue burden would be imposed on Google for complying with an unlawful order, Google failed to point to any evidence of the Order's unlawfulness, apart from the perpetual nature of the nondisclosure Order. The court then modified the Order to limit the nondisclosure provision to 90 days with the ability of the government to petition for an extension of 60 days.

As described above, Judge [redacted] correctly interpreted the unambiguous language of the SCA. Google has no meritorious statutory basis to move to modify the non-disclosure and sealing provisions of the Order. Judge [redacted] committed no error in denying Google's motion in part and granting it in part to limit the duration of the non-disclosure provision. Thus, the Orders are not clearly erroneous or contrary to law.

C. The Order Is Constitutional.

a. The Subscribers Have No Meritorious Statutory or Constitutional Claims

Google also claims that the Order, which seeks limited subscriber information and transactional records but not the content of any communications, "may raise significant constitutional and statutory issues." Google Mot. at 12. First, Google argues that the Court should exercise its discretion to modify the Order to allow Google to give notice to the [redacted] subscriber, who may wish to assert -- as he has with respect to the Twitter Order -- statutory and constitutional arguments, including alleged violations of the First and Fourth Amendment. Google Mot. at 12-13 (citing Roche Decl. Ex. 3).

2703(d) order. Indeed, Google customers know about and consent to lawfully issued legal process. *See* Google Privacy Policy, http://www.google.com/privacy/privacy-html (last visited Feb. 28, 2011) (explaining that Google "shares personal information with other companies or individuals outside of Google" when Google has "a good faith belief that access, use, preservation, or disclosure of such information is reasonable necessary to . . . satisfy any applicable law, regulation, legal process or enforceable governmental request.").

For the reasons explained in the Government's Opposition to Google's Motion (Roche Decl. Ex. 7), incorporated here by reference, the Order is proper, and neither the [redacted] subscriber nor Google can mount a viable challenge. Further, any additional arguments that the [redacted] subscriber has raised in opposition to the Twitter Order (Google Mot. at 12-13), and may seek to raise in this case, lack merit for the reasons explained in the government's Objection to the Motion of the Three Twitter Subscribers to Vacate Order of December 14, 2010, Under § 2703(d). Govt. Ex. 2 (*ex parte*).[7]

In short, even if the [redacted] subscriber had notice of the Order, he would not be entitled to bring a wide-ranging motion to vacate it. Although the SCA authorizes some judicial remedies for subscribers who seek to challenge orders, *see* 18 U.S.C. § 2704(b), these remedies apply to legal process seeking the *content* of the subscriber's communications and do not apply to legal process for business records under 18 U.S.C. § 2703(d), like the Order here. As noted above, Congress did not provide subscribers with wide-ranging remedies that would allow them to challenge non-content orders, such as the Order here, for alleged nonconstitutional violations of the SCA. *See* 18 U.S.C. § 2708.

Even if the [redacted] subscriber had standing to assert a constitutional claim and wished to assert a First Amendment challenge, the claim would be meritless. As the Supreme Court has recognized, "neither the First Amendment nor any other constitutional provision protects the average citizen from disclosing to a grand jury information that he has received in confidence." *Branzburg v. Hayes*, 408 U.S. 665, 682 (1972). This is true even if WikiLeaks is a journalistic enterprise, which Google claims is a matter of public debate but does not allege, and which the government does not concede. Google Mot. at 4. As the Supreme Court has concluded, "the

[7] Pending Magistrate [redacted] ruling on the unsealing of this pleading, the government files it in this case *ex parte* and under seal in an abundance of caution.

Constitution does not . . . exempt the newsman from performing the citizen's normal duty of appearing and furnishing information relevant to the grand jury's task." *Id.* at 691. Indeed, journalists have no special privilege to resist compelled disclosure of their records, absent evidence that the government is acting in bad faith. *See In re Shain*, 978 F.2d 850, 852 (4th Cir. 1992); *see also Univ. of Pennsylvania v. E.E.O.C.*, 493 U.S. 182, 201 n.8 (1990) (implying that "the bad-faith exercise of grand jury powers" is the only basis for a First Amendment challenge to a subpoena).

The [redacted]r subscriber here could not quash the Order because he could not show that the government has acted in bad faith or with the intent to harass, either in conducting its criminal investigation or in obtaining the Order. *See United States v. Steelhammer*, 539 F.2d 373, 376 (4th Cir. 1976) (Winter, J., dissenting), *adopted by the court en banc*, 561 F.2d 539, 540 (4th Cir. 1977) ("[T]he record fails to turn up even a scintilla of evidence that the reporters were subpoenaed to harass them or to embarrass their newsgathering abilities . . ."). The government described the nature of its investigation in its application for the Order, and a neutral magistrate had an opportunity to review it before issuing the Order. The magistrate concluded that the Order was proper because the government "offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation." Roche Decl. Ex. 1; *see also* 18 U.S.C. § 2703(d).

The [redacted] subscriber's potential challenges to the Order are even weaker because of the Order's limited scope. The Order requires Google to disclose certain business and transactional records about the [redacted] subscriber's account. *See* Roche Decl. Ex. 1. The [redacted] subscriber has no reasonable expectation of privacy under the Fourth Amendment in these records. *See*

United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010) (individual has no subjective or reasonable expectation of privacy in his internet and phone "subscriber information," i.e. his name, email address, telephone number and physical address) (citing *Smith v. Maryland,* 442 U.S. 735, 744 (1979) and *United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008)). It is difficult to imagine how any First Amendment rights of the Subscriber could be infringed by Google's disclosure of business records such as these, and Google has not asserted otherwise.

b. Google Has No Meritorious First Amendment Claims

Google claims that the Order's non-disclosure provisions constitute a prior restraint on its speech that violates Google's own First Amendment rights. Google Mot. at 13 Google is wrong. Courts regularly issue sealing orders, protective orders, and other non-disclosure orders that preclude private parties from discussing matters before the court. *See e.g., In re Application of United States of America for an Order Pursuant to 18 U.S.C. § 2703(d) Directed to Cablevision Systems Corp.,* 158 F.Supp.2d 644, 648-49 (D. Md. 2001) (holding that the Electronic Communications Privacy Act implicitly repealed provisions of the Cable Communications Policy Act that required notice to a subscriber of a cable company service of a court order directing disclosure of the subscriber's personal information) (citing in support, 12 U.S.C. § 3409 (authorizing delayed notice for financial institutions); 18 U.S.C. §§ 2511(2)(a)(ii) (prohibiting disclosure of wire interceptions); § 3123(d) (prohibiting disclosure of pen registers or trap and trace devices)).

Indeed, 18 U.S.C. § 2705(b) was enacted almost twenty-five years ago, and to the government's knowledge, no court has ever held that its procedures fail to comply with the requirements of the First Amendment. *See* Electronic Communications Privacy Act of 1986, PL 99-508, § 201, 100 Stat. 1848 (1986). Furthermore, Judge [redacted] Order 2, adopting a modified form of the government's proposal, limited the non-disclosure period to 90 days, subject to a

possible court-ordered extension of no more than 60 days. Even Google recognizes that "nondisclosure requirements of a *limited* duration are not uncommon in normal investigations." Google Mot. at 14. *See In re Sealing and Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F.Supp.2d 876, 881-82, 895 (S.D.Tex. 2008) (recognizing that "restrictions on speech and public access are presumptively justified while the investigation is ongoing" and permitting a 180-day period for non-disclosure with a provision to allow the government to move for extension).

For all the reasons set forth above, the Order, including its non-disclosure and sealing requirements, as amended by Order 2, is proper in every respect. Google has no basis to challenge the Order under the statute or the constitution. Judge [redacted] committed no error, and the Orders are neither clearly erroneous nor contrary to law.

III. The Disclosure of the Twitter Order Does Not Justify Disclosure of This Order, Particularly When Unsealing the Twitter Order Already Has Seriously Jeopardized the Investigation.

Google argues that because the government voluntarily agreed to the unsealing and disclosure of the Twitter Order, the Court should do so here, particularly because both orders are part of the WikiLeaks investigation, the existence of which has been publicly acknowledged. *See* Google Mot. at 9-12. Google is mistaken. The government's decision to voluntarily move to unseal and permit notice of the Twitter Order was based upon its particularized assessment of the continuing need for sealing and notice preclusion. This decision was a reasonable exercise of the government's prosecutorial discretion and should not bind the government as to other orders.

Moreover, the unsealing and disclosure of the Twitter Order already has seriously jeopardized the investigation despite the publicly acknowledged investigation. Unsealing and allowing disclosure by Google will exacerbate the harm. Indeed, in light of the events that

followed the unsealing and disclosure of the Twitter Order, had the government known then what it does now, it would not have voluntarily filed the motion to authorize it.

These events are detailed in the Government's Response to the Google Motion (Roche Decl. Ex. 7) and are incorporated here by reference. They show how the circumstances have changed in the investigation since – and in part as a result of – the government's decision to unseal and disclose the Twitter Order. In short, the disclosure and unsealing of the Twitter Order has seriously jeopardized the investigation.

First, the government confirmed that despite the public nature of the investigation, disclosure of the particular investigative step at issue in the Twitter Order increased the risk that witnesses and targets would alter their modes of communication to evade future investigative efforts. One reason for sealing and ordering non-disclosure under Section 2705 in the Twitter case, as well as here, is that disclosure would seriously jeopardize the investigation because it might cause suspects to change their patterns of behaviour and notify confederates to change their patterns of behaviour. Once the Twitter Order was unsealed, the [redacted] subscriber to Twitter announced a change in his behavior and made a general announcement to others who might potentially have evidence relevant to the investigation by posting a message to Twitter on January 7, 2011, that stated "Do not send me Direct Messages – My Twitter account contents have apparently been invited to the (presumably Grand Jury) in Alexandria." *See* Roche Decl. Ex. 7, Gov't Ex. 2

Second, the disclosure and unsealing also presented the unforeseen risk of witness intimidation. Google belittles this risk. Protecting witnesses from public exposure, however, encourages them to voluntarily come forward and to testify fully without fear of retribution. These two core principles underlie the need for secrecy in the grand jury process. *See United*

States v. Reiner, 934 F. Supp. 721, 723 (E.D.Va. 1996) (citing *Douglas Oil Co. v. Petrol Stops Northwest*, 441 U.S. 211, 219 (1979)). Other providers – who are potential witnesses - may fear that public exposure of their willing compliance with court orders relating to this investigation will hurt their reputation and feel pressure to challenge non-disclosure orders. Providers might also fear retribution beyond damage to goodwill. The press has widely reported that companies who withdrew their services from WikiLeaks have been cyber attacked. Charlie Savage, *F.B.I. Warrants Into Service Attacks by WikiLeaks Supporters*, NY Times, http://www.nytimes.com/2011/01/28/us/28wiki.html

Third, repeatedly unsealing and disclosing process during an ongoing investigation presents a heightened risk of jeopardizing the investigation, potentially revealing each step the government has taken and highlighting those that have yet to be taken. The subjects of the investigation do not yet know what the government knows. And each piece of the investigative puzzle revealed to them provides them with a better picture.

Finally, the disclosure and unsealing of the Twitter Order has already resulted in harassment that disrupted the investigation by diverting resources and attention. A similar reaction can be expected if disclosure and unsealing is authorized here.

Just as the government then underestimated the degree of damage that would result from the unsealing and disclosure of the Twitter Order, Google underestimates the likely damage that would attend unsealing and disclosure in this matter. For all of these reasons, the government has not agreed to disclosure of the Order. The non-disclosure and sealing provisions of the Order remain legally justified, and disclosure is not in the best interest of the investigation. Judge [redacted] committed no error in so concluding and the Orders are not clearly erroneous or contrary to law.

Conclusion

In conclusion, the Court should overrule Google's objections. The Orders, including the limited sealing and non-disclosure provisions, remain warranted more than ever. Unsealing and disclosure of the Order would significantly jeopardize the investigation. Finally, the United States respectfully suggests that a hearing is not necessary in this case. The legal issues are not novel, and oral argument would not aid the Court in reaching its decision.

Respectfully Submitted,

[redacted]
United States Attorney

By: [redacted]
Assistant United States Attorney

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing pleading was delivered on this 28th day of February 2011 to the Clerk's Office and that service will be made on the following individuals by electronic mail and otherwise:

John K. Roche, Esquire
Perkins Coie LLP
700 13th St., N.W., Suite 600
Washington, D.C. 20005-3960
PHONE: 202.434.1627
FAX: 202.654.9106
E-MAIL: JRoche@perkinscoie.com

Assistant United States Attorney

GOVERNMENT EXHIBIT 2
(1:11DM00003, DKT. #21)

UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE §2703(d) ORDER RELATING TO TWITTER ACCOUNTS: WIKILEAKS, ROP_G; IOERROR; AND BIRGITTAJ	)	MISC. NO. 10GJ3793 No. 1:11DM3 (Judge Buchanan) Hearing: February 15, 2011 10:30 a.m. **UNDER SEAL**

GOVERNMENT'S OBJECTION TO MOTION OF THREE TWITTER SUBSCRIBERS TO VACATE ORDER OF DECEMBER 14, 2010, UNDER § 2703(d)

The United States of America, by and through Neil H. MacBride, United States Attorney, Eastern District of Virginia, and John S. Davis, Assistant United States Attorney, objects as follows to the Motion of Real Parties in Interest Jacob Appelbaum, Birgitta Jonsdottir, and Rop Gonggrijp to Vacate December 14, 2010 Order:

I. ***Background***

On December 14, 2010, this Court entered a sealed order (the Order) pursuant to 18 U.S.C. § 2703(d) directing Twitter, Inc., to disclose certain non-content records and other information pertaining to Twitter accounts, including those identified as rop_g; ioerror; and birgittaj. For each account, the Order specified the following customer or subscriber information, for the period November 1, 2009, to the date of the Order:

1. subscriber names, user names, screen names, or other identities;
2. mailing addresses, residential addresses, business addresses, e-mail addresses, and other contact information;
3. connection records, or records of session times and durations;
4. length of service (including start date) and types of service utilized;
5. telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

6. means and source of payment for such service (including any credit card or bank account number) and billing records.

The Order also identified additional records, for the same Twitter accounts and same time period:

1. records of user activity for any connections made to or from the Account, including the date, time, length, and method of connections, data transfer volume, user name, and source and destination Internet Protocol address(es);
2. non-content information associated with the contents of any communication or file stored by or for the account(s), such as the source and destination email addresses and IP addresses.
3. correspondence and notes of records related to the account(s).

On January 5, 2011, this Court unsealed the Order (but no other document in this matter), and authorized Twitter to disclose it. Twitter thereafter gave notice of the Order to the affected account holders, including the three "real parties in interest," who are movants here: Jacob Appelbaum (associated with ioerror), Birgitta Jonsdottir (associated with birgittaj), and Rop Gonggrijp (associated with rop_g) (collectively, the Subscribers).

After discussions with counsel, on January 12, 2011, the government agreed with Twitter to a narrowing of the terms of the Order, reducing the number of records to be disclosed.[1] On

[1]On or about January 12, 2011, the government informed Twitter and the Subscribers that it agreed to the following with respect to the Order: 1. The government expected Twitter to provide information covered by the Order only for the four listed Twitter accounts (Wikileaks, rop_g, ioerror, and birgiittaj) between November 15, 2009 and June 1, 2010; 2. to the extent Twitter has no information responsive to certain parts of the Order, for example credit card information, it need not provide such information; 3. the government had not sought and did not expect to receive the contents of any communications; 4. the government did not expect Twitter to provide records that would be unusually voluminous in nature or would otherwise cause an undue burden to produce. Twitter should let the government know if it believed any portion of the Order would be unduly burdensome after consultation with its engineers. For example, the government did not expect Twitter to produce the records of user activity for any connections to or from the Account relating to public followers of a Twitter account, Apache logs, or replies to Twitter feeds; 5. the government and Twitter understood that the records of user activity for any connections to or from the Account would include the IP addresses of the Account holder's

January 26, 2011, the Subscribers moved to vacate the Order, citing a variety of statutory and constitutional grounds. The government hereby objects to the Subscribers' motion.

II. *Argument*

A. Section 2703(d) Does Not Authorize the Subscribers to Challenge a "Non-Content" Order For an Alleged Non-Constitutional Violation of the Statute, and, in Any Event, This Court Has Already Determined That the Order is Based Upon "Specific and Articulable Facts."

The Subscribers first argue that no "specific and articulable facts" demonstrate that the Twitter records identified in the Order are "relevant and material" to a criminal investigation, as § 2703(d) requires. Although they are not privy to the Order's factual basis (which remains sealed), the Subscribers contend that because their "Tweets" covered a "broad range of non-WikiLeaks topics," the records identified in the Order necessarily include data "that has no connection whatsoever to WikiLeaks and cannot be relevant or material to any investigation." (Mot. Vacate at 6-7.) Accordingly, say the Subscribers, the Order must be vacated and the government's application disclosed, to allow them "a fair opportunity to challenge the Government's assertions and highlight any material misstatements or omissions." (Mot. Vacate at 7.)

---

logins; and 6. the government believed that the records of user activity for any connections to or from the Account would include non-content information relating to direct messages between the four accounts listed in the Order (Wikileaks, rop_g, ioerror, and birgiittaj), for example non-content information reflecting the fact that a message was passed between such accounts. The government also understood that Twitter was looking into whether it agreed that the Order covered such connection records and whether it was possible to produce them from an engineering standpoint. The government confirmed that it was not seeking any information (content or non-content) relating to direct messages except those exchanged among any of the four accounts listed in the Order.

The Subscriber's statutory claim is meritless. As this Court has already determined, the government's application for the Order (the Application) satisfied the governing standard by alleging "specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation." (Order at 1.) The Order is therefore fully compliant with § 2703(d), and the Court should reject the Subscribers' speculation that the Application "likely contains material errors or omissions" that render it insufficient. (Mot. Vacate at 1.)

Several additional reasons require rejection of the Subscribers' § 2703(d) argument. In the first place, the Subscribers cannot move to vacate the Order on statutory grounds. The Order was issued under 18 U.S.C. § 2703(d), which is part of the Stored Communications Act (18 U.S.C. §§ 2701-12) (the SCA). That Act expressly prohibits the improvising of remedies. Specifically, Congress provided that "[t]he remedies and sanctions described in [the SCA] are the only judicial remedies and sanctions for nonconstitutional violations of [the SCA]." 18 U.S.C. § 2708; *see United States v. Clenney*, No. 09-5114, slip op. at 13 (4th Cir. Feb. 3, 2011). Thus, because the Subscribers' first argument alleges a nonconstitutional violation of § 2703(d), they may invoke only the "judicial remedies" described in the SCA to address the putative illegality. Accordingly, in challenging the Order based on an alleged violation of the § 2703(d) standard, the Subscribers must identify authority in the SCA that permits such a motion in the first place. But the Subscribers have failed to do so, and with good reason – the SCA does not authorize them to move to vacate the Order for a nonconstitutional § 2703(d) violation.

The SCA provides only two ways to challenge a § 2703(d) order. First, the "service provider" may move to quash or modify the 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). This remedy would theoretically be available to Twitter, the named service provider, but it is not available to the Subscribers.

Second, a "subscriber or customer" may move to vacate an order, but only under certain conditions, including when the order seeks the contents of that subscriber or customer's communications. *See* 18 U.S.C. § 2704(b)(1)(A) (motion to vacate must state "that the applicant is a customer or subscriber to the service from which the contents of electronic communications maintained for him have been sought"). Here, of course, the Order seeks only "non-content" records and information about the Subscribers' Twitter accounts.

Notably, subscribers are not entitled to notice that the government has sought disclosure of non-content information under § 2703(c), as the government has here. *See* 18 U.S.C. § 2703(c)(3) ("A governmental entity receiving records or information under this section is not required to provide notice to a subscriber or customer"). On the other hand, if the government were seeking content information under Section 2703(b), notice (albeit notice that may be delayed) is required unless a search warrant is obtained. *See* 18 U.S.C. § 2703(b)(1). Since Congress required that subscribers be notified only when content is disclosed, it makes sense that Congress provided subscribers with the ability to contest only such disclosures. *See Clenney*, No. 09-5114, slip op. at 12 (noting that statute "draws a distinction between the content of a communication and the records pertaining to a communication service account").[2]

[2]If the Subscribers have been aggrieved by a wilful violation of the SCA, they may sue the United States for money damages under 18 U.S.C. § 2712. Challenging the Order in the manner chosen here, however, is simply not among the options Congress authorized.

The above-described legal framework comports with practical demands and with common sense. Pre-indictment challenges can interfere with ongoing criminal investigations, and Congress carefully and appropriately tailored the ability to challenge the government's acquisition of non-content information. Because the Subscribers cannot avail themselves of the only remedies set forth in the SCA, the Subscribers have no basis to move to vacate the Order on statutory grounds.

Moreover, even assuming that the procedures in § 2704(b) were available to the Subscribers, any challenge to the Order under § 2704(b) would fail. That section provides that a motion to vacate must be denied if "there is a reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry." 18 U.S.C. § 2704(b)(4). In this case, any motion to vacate the Order under § 2704(b) would be denied because in the Order this Court has already concluded that the government satisfied the higher § 2703(d) standard of providing "specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation."[3]

[3]By its terms, section 2704(b) does not permit customers to contest whether the records sought by a § 2703(d) order are *material* to an investigation, and legislative history confirms that Congress intended not to provide customers with this authority. As described above, until 1994, the standard for issuing a § 2703(d) order was identical to that for evaluating a § 2704(b) challenge: in both cases, courts had to determine whether the records sought were "relevant to a legitimate law enforcement inquiry." *See* Pub.L. 99-508, Title II, § 201, Oct. 21, 1986, 100 Stat. 1861. In 1994, Congress changed the § 2703(d) standard to require that the records be "relevant and material to an ongoing criminal investigation," but left § 2704 unchanged, thereby precluding customers from employing the new materiality standard in § 2704 litigation. *See* Pub.L. 103-414, Title II, § 207(a), Oct. 25, 1994, 108 Stat. 4292.

Lacking a legitimate statutory remedy, the Subscribers instead ask the Court to review its own issuance of the Order *de novo* and evaluate, again, whether the Application meets the "specific and articulable facts" standard in 18 U.S.C. § 2703(d). (Mot. Vacate at 4-6.) For all the reasons set forth above, the SCA does not allow the Subscribers to seek such a review. Further, even if this Court were to reconsider the Application, it would find it more than sufficient to meet the § 2703(d) standard. Specifically, as narrowed by the government's agreement with Twitter, the Order seeks certain non-content business records that may be obtained via a subpoena with no threshold showing to the court, namely (a) subscriber information, including the subscriber's name, address, connection records, subscriber number, and length of service; and (b) correspondence and records relating to an account. These types of business records can be routinely obtained from providers by subpoena, and the Subscribers have no reasonable expectation of privacy in them. *See Clenney*, No. 09-5114, at 11 (recognizing that under § 2703(c)(2) government can bypass warrant or court order procedures "and simply subpoena the records if it seeks only basic subscriber information, such as the name and address of the customer and telephone call logs"); *United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010) (individual had no subjective or reasonable expectation of privacy in his internet and phone "subscriber information," i.e., his name, email address, telephone number and physical address, when he voluntarily conveyed this information to internet and telephone companies) (citing *Smith*, 442 U.S. at 744, and *United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008)).

Further, the following non-content information is the only material sought from Twitter that required the government to show specific and articulable facts to support a reason to believe

that such information was relevant and material to an ongoing criminal investigation. (The Application adequately established this, as this Court has already found.) As narrowed by the government's agreement, see note 1 *supra*, the Order requires disclosure of the following non-content information:

1. Records of user activity for connections made between the four listed accounts (to or from), including IP addresses (which are akin to telephone numbers for a computer), and dates and times (this would include the IP addresses of direct (private) twitter messages between the relevant accounts, for example); and
2. non-content information associated with the contents of communications or stored files (this would include, for example, the IP address of the recipient of a direct message to the extent that recipient is also an account user).

At least one court has ruled that "the 'specific and articulable facts' standard derives from the Supreme Court's decision in *Terry*." *United States v. Perrine*, 518 F.3d 1196, 1202 (10th Cir. 2008) (*citing Terry v. Ohio*, 392 U.S. 1 (1968)). It follows that "this standard is a lesser one than probable cause." *In re Application of United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to Government*, 620 F.3d 304, 313 (3d Cir. 2010) (*Third Circuit Opinion*); *see United States v. Warshak*, — F.3d —, 2010 WL 5071766, at *16 (6th Cir. Dec. 14, 2010) (noting "diminished standard that applies to § 2703(d) applications"); *see also* S. Rep. No. 99-541, at 44-45 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3598-99. The *Terry* standard is met "when an officer 'point[s] to specific and articulable facts which, taken together with rational inferences from those facts, evince more than an inchoate and unparticularized suspicion or hunch of criminal activity.'" *United States v. Mason*, 628 F.3d 123, 128 (4th Cir. 2010) (*quoting United States v. Branch*, 537 F.3d 328, 336 (4th Cir. 2008)).

The Subscribers imply that the "specific and articulable facts" standard is more onerous

than the *Terry* rule (Mot. Vacate at 5), but they identify no court that has adopted this position, and the government is aware of none. The presence of the word "material" in 18 U.S.C. § 2703(d) does not transform the § 2703(d) standard into one that requires a showing that the records sought are "vital," "highly relevant," or "essential," as the Subscribers suggest. (Mot. Vacate at 5.) The Subscribers' contrary argument is based on cases that discuss "materiality" in contexts very different from § 2703(d). *See* (Mot. Vacate at 5); *United States v. Valenzuela-Bernal*, 458 U.S. 858, 867-73 (1982) (evaluating whether deportation of potential witnesses violated defendant's constitutional rights); *Roviaro v. United States*, 353 U.S. 53, 62-65 (1957) (evaluating whether government could withhold identity of undercover informer); *United States v. Smith*, 780 F.2d 1102, 1109 (4th Cir. 1985) (evaluating whether government could preclude defendant from introducing classified information at trial). Here, the facts described in the Application fully meet the *Terry* standard and therefore satisfy § 2703(d)'s requirements. *Mason*, 628 F.3d at 128.

Further, there is no merit to the Subscribers' claim that the records described in the Order cannot be "relevant and material to an ongoing criminal investigation" simply because some of them relate to communications "that have nothing whatsoever to do with WikiLeaks." (Mot. Vacate at 6.) By the Subscribers' logic, the government could never use a § 2703(d) order to obtain email transaction logs or phone bills unless the government could show that every email or phone call related directly to the crime under investigation. And their position has radical practical implications. Should providers be required in the first instance to review individual transaction records to determine relevancy? Providers are singularly ill-equipped to determine precisely what information would be relevant to an ongoing investigation. The government is

aware of no court that has adopted such a restrictive and impractical view of § 2703(d). Nor is such a view required by law. *See In re Subpoena Duces Tecum*, 228 F.3d at 348-49 (in explaining that subpoenas are less intrusive than search warrants and therefore require a lower standard, noting that "[t]he Government cannot be required to justify the issuance of a grand jury subpoena by presenting evidence sufficient to establish probable cause because the very purpose of requesting the information is to ascertain whether probable cause exists") (quoting *United States v. R. Enterprises, Inc.*, 498 U.S. 292 (1991)). Contrary to the Subscribers' assertions, the Order requires the production of very limited transactional information that is directly relevant and material to the ongoing criminal investigation. This is especially true since with the government's agreement the Order is limited to connection information between the identified account holders.

In summary, because the SCA strictly limits the remedies available to subscribers whose non-content information is sought, the Subscribers cannot challenge this Court's finding under § 2703(d) that "specific and articulable facts" support the Order. And even if they could mount such a challenge, it would fail, since the facts in the Affidavit are more than sufficient.

B. The Order Does Not Infringe Upon Any First Amendment Rights Held by the Subscribers.

The Subscribers next protest that the Order, which seeks limited subscriber information, such as names and addresses, and transactional records, such as connection data, all of which are business records of Twitter but not the content of the Subscribers' communications, "threatens the Parties' protected First Amendment rights." (Mot. Vacate at 7.)[4] The Subscribers accuse the

[4]Neither Mr. Gonggrijp nor Ms. Jonsdottir appears to be a United States citizen. Additionally, no information, whether in their filing or within the government's knowledge, suggests that either of them maintained a significant continuing presence in the United States during the period of the

government of undertaking a "fishing expedition" that may chill their rights "to speak freely and associate with others." (Mot. Vacate at 8.) They conclude that under the First Amendment, unless the government can show that the information sought "would further a compelling interest," and that its request is "the least restrictive way to serve that interest," the Order must be vacated. (Mot. Vacate at 10.)

But the Subscribers' argument is long on rhetoric and short on facts demonstrating an actual "chill" on First Amendment freedoms. In reality the Order, which is not conceptually different from a routine subpoena seeking telephone subscriber information and toll records from a telephone company, in no way inhibits the exercise of First Amendment rights.

Moreover, the Parties cannot demonstrate that they are entitled to "particular scrutiny" of the Order based on alleged First Amendment interests. (Mot. Vacate at 8.) The Fourth Circuit has specifically declined to apply the "substantial relationship" test, which balances First Amendment freedoms against the government's interest in investigating crime, to a grand jury subpoena seeking corporate records of a distributor of sexually explicit films. *In re Grand Jury 87-3 Subpoena Duces Tecum*, 955 F.2d 229, 234 (4th Cir. 1992). Instead, the court directed the district court to "balance the possible constitutional infringement and the government's need for

---

investigation. There is a legitimate question whether the rights under the Constitution of non-citizen, non-national, non-residents of the United States are substantially identical to those of citizens, residents, or individuals acting within the United States. *See, e.g., United States v. Verdugo-Urquidez*, 494 U.S. 259, 265 (1990) (textual analysis of Constitution "suggests that 'the people' protected by the Fourth Amendment, and by the First and Second Amendments . . . refers to a class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community"). Mr. Gonggrijp and Ms. Jonsdottir do not address this threshold question before making arguments that imply that the First and Fourth Amendments apply to them just as they do to Mr. Appelbaum (who is a United States citizen). In any event, for the reasons set forth *infra*, none of the Subscribers identifies a constitutional violation warranting the extraordinary relief that they seek.

documents" when ruling on the motion to quash, "on a case-by-case basis and without putting any special burden on the government." *Id.*

Doubtless, as the Subscribers assert, the freedoms of speech and association constitute important rights protected by the First Amendment. But, setting aside legal platitudes, the Subscribers fail to present a cognizable First Amendment claim. The irony presented in this case is that the Subscribers publicly posted their Tweets -- the contents of their messages -- on the Internet. Information about the Subscribers' Twitter followers was also public, since the followers of the Subscribers' Tweets posted their replies on the Internet. Thus, although the Subscribers claim otherwise, the government has not embarked on a "fishing expedition into information about their postings." (Mot. Vacate at 8.) Nothing remains to fish for, since the Subscribers and their associates have already made their postings available for all the world to see, and can have no expectation of privacy in them. Nor does the government seek the contents of any of the Subscribers' private direct messages (akin to private Internet chats), or seek to identity others with whom the Subscribers communicated by direct messages. (Mot. Vacate at 8.) As narrowed by the government's agreement with Twitter, the Order's scope extends only to non-content connection records for past communications involving the identified account holders. It does not seek prospective connection records, or attempt to identify the Subscribers' associates. It does not control or direct the content of the Subscribers' speech, or restrain, punish or burden any speech or association in which the Subscribers may have engaged. For good reason, the Subscribers fail to explain how the Order chills their freedom of speech or association: they cannot. *See Univ. of Pennsylvania v. E.E.O.C.*, 493 U.S. 182, 197-98 (1990) (subpoena for academic papers did not impose content-based or direct burden on university);

Branzburg v. Hayes, 408 U.S. 665, 682, 691 (1972) (requiring reporter to comply with subpoena "involves no restraint on what newspapers may publish, or on the type or quality of information reporters may seek to acquire," nor does it threaten "a large number or percentage of all confidential news sources").

Thus, even if the "substantial relationship" test were required in the Fourth Circuit -- which it is not – since enforcement of the Order will not chill speech or association, that test would not apply. *In re Grand Jury 87-3 Subpoena Duces Tecum*, 955 F.2d at 234 (following *Branzburg* and *University of Pennsylvania*). To the extent that the provider, Twitter, stands in the same shoes as an ordinary citizen before this Court, "neither the First Amendment nor any other constitutional provision protects [it] from disclosing to a grand jury information that [it] has received in confidence,"[5] absent a showing of harassment or bad faith. *Branzburg*, 408 U.S. at 682, 707; *Univ. of Pennsylvania*, 493 U.S. at 201 n.8 (1990) (implying that "the bad-faith exercise of grand jury powers" is the only basis for a First Amendment challenge to a subpoena); *In re Shain*, 978 F.2d 850, 852 (4th Cir. 1992).

Finally, the Subscribers do not allege – and cannot show – that the government has acted in bad faith, either in conducting its criminal investigation or in obtaining the Order. The government described the nature of its investigation in its Application, allowing the Court to assess the legitimacy of the case before deciding to issue the Order. The government's decision

[5]Most cases that evaluate First Amendment challenges to the compelled disclosure of documents involve subpoenas, rather than court orders. Court orders issued under 18 U.S.C. § 2703(d), such as the Order, are similar to subpoenas because they also require the disclosure of documents, but they are arguably more protective of citizens' interests because they are subject to prior judicial review and require a higher factual showing for issuance. Accordingly, a party attempting to challenge a § 2703(d) court order should be subject to standards that are at least as stringent as those applied to a motion to quash a subpoena.

to pursue the particular records described in the Order was also subject to oversight by this Court, which concluded that the Order was warranted because the government "offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). The government has acted in good faith throughout, and there is no evidence that either the investigation or the Order is intended to harass the Subscribers or anyone else. *See In re Grand Jury* 87-3, 955 F.2d at 233 n.3 (noting that there was no allegation of grand jury bad faith); *United States v. Steelhammer*, 539 F.2d 373, 376 (4th Cir. 1976) (Winter, J., dissenting), *adopted by the court en banc*, 561 F.2d 539, 540 (4th Cir. 1977) ("[T]he record fails to turn up even a scintilla of evidence that the reporters were subpoenaed to harass them or to embarrass their newsgathering abilities . . ."). Accordingly, the Subscribers have no colorable First Amendment claim justifying vacation of the Order.

C. Because the Subscribers Have No Expectation of Privacy in Their IP Addresses Provided to Twitter, the Order Does Not Violate Their Fourth Amendment Rights.

The Court should likewise reject the Subscribers' claim that the Order threatens their Fourth Amendment rights. The Subscribers identify only one aspect of the Order that supposedly implicates such rights: its directive that Twitter produce the Internet Protocol ("IP") addresses that the Subscribers used to log in to their Twitter accounts at particular dates and times. (Mot. Vacate at 10.) According to the Subscribers, this IP address information, in connection with the dates and times of the account logins, implicates the Fourth Amendment because it "could allow the government to discern the physical location of the parties at the exact time they were

publishing on Twitter." *Id.* However, even assuming for argument's sake that the Subscribers have standing to bring a Fourth Amendment challenge to the Order, the Subscribers have no Fourth Amendment interest in IP address information, and the Order cannot not be vacated on that ground.

IP addresses are analogous to telephone numbers. *See United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008). Just as every telephone is assigned a number that phone companies use to route calls, every computer directly connected to the Internet is assigned an IP address that "serves as the routing address for email, pictures, requests to view a web page, and other data sent across the Internet." *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 409 (2d Cir. 2004). "Like telephone numbers, . . . IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party's servers." *Forrester*, 512 F.3d at 510. Accordingly, the government's acquisition of IP address information is properly analyzed using the same legal framework that applies to the government's acquisition of phone numbers. *See id.* (concluding that real-time collection of IP addresses of websites visited by Internet user was "constitutionally indistinguishable" from the use of a pen register to collect numbers dialed from a phone line).

Because IP addresses are analogous to phone numbers and should be governed by the same legal rules, *Smith v. Maryland*, 442 U.S. 735 (1979), disposes of the Subscribers' Fourth Amendment claim. In *Smith*, the Supreme Court concluded among other things that telephone users had no reasonable expectation of privacy in the telephone numbers they dialed because they "voluntarily conveyed numerical information to the telephone company" and thereby "assumed the risk that the company would reveal to police the numbers . . . dialed." 442 U.S. at 744. This

conclusion is consistent with the general rule that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 743-44 (citing cases); *see also United States v. Miller*, 425 U.S. 435, 440 (1976) (bank depositor had no "legitimate expectation of privacy" in financial information "voluntarily conveyed to . . . banks and exposed to their employees in the ordinary course of business"); *Bynum*, 604 F.3d at 164 (internet user had no legitimate expectation of privacy in subscriber information that he voluntarily conveyed to his internet company). Just as telephone users voluntarily transmit phone numbers to their phone providers, the Subscribers voluntarily transmitted their IP addresses to Twitter to gain access to their Twitter accounts, thereby assuming the risk that Twitter would reveal the addresses to law enforcement agents. *See Forrester*, 512 F.3d at 510. Indeed, Twitter's Privacy Policy places all users on notice that Twitter servers "automatically record information ('Log Data') created by your use of the Services," and specifies that this Log Data "may include information such as your IP address." Twitter Privacy Policy, http://twitter.com/privacy (last visited February 1, 2011). Accordingly, based on the Supreme Court's reasoning in *Smith*, the Subscribers cannot now claim a reasonable expectation of privacy in Twitter's records of their IP addresses.[6]

To the government's knowledge, no court has concluded that Internet users have a

[6]Even if the Subscribers somehow had a reasonable expectation of privacy in their IP address information, the Order would not be improper under the Fourth Amendment. *See Smith*, 442 U.S. at 744 ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities."); *S.E.C. v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984) (past Supreme Court rulings "disable respondents from arguing that notice of subpoenas issued to third parties is necessary to allow a target to prevent an unconstitutional search or seizure of his papers"); *Okla. Press Pub. Co. v. Walling*, 327 U.S. 186, 208 (1946) (explaining Fourth Amendment requirements for subpoenas).

reasonable expectation of privacy in IP address records. Indeed, at least two courts of appeals have affirmatively held that Internet users have no reasonable expectation of privacy in IP address information.[7] *See Forrester*, 512 F.3d at 510 ("[E]-mail and Internet users have no expectation of privacy in . . . the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information."); *United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010) ("[N]o reasonable expectation of privacy exists in an IP address, because that information is also conveyed to and, indeed, from third parties, including ISPs."). This Court should adopt the reasoning of these cases and hold that the Subscribers lack a reasonable expectation of privacy in their IP address information.

Moreover, there is no merit to the Subscribers' suggestion that the Court should depart from these cases and conclude that IP address records deserve Fourth Amendment protection because they "could allow the government to discern the physical location of the [Subscribers] at the exact time they were publishing on Twitter." (Mot. Vacate at 10.) Business records do not become privileged merely because they contain information that might enable the government to

---

[7]The Subscribers do not address these cases and instead imply in a footnote that only opinions "specifically addressing Twitter data" are directly on point. (Mot. Vacate at 12 n.10.) But there is no legal basis for distinguishing Twitter's IP address records from the IP address records of any other Internet service provider. In any event, cases that analyze the collection of IP address information are much more relevant to the Subscribers' Fourth Amendment argument than the cases cited by the Subscribers in the same footnote, which evaluate government searches of computers seized from private homes and government efforts to obtain the content of email messages. *See Trulock v. Freeh*, 275 F.3d 391, 402-03 (4th Cir. 2001) (consent-based search of home, computer, and computer files); *United States v. Mann*, 592 F.3d 779, 786 (7th Cir. 2010) (warrant-based search of computers seized from defendant's home); *United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999) (same); *United States v. Warshak*, --- F.3d ---, 2010 WL 5071766, at *11, *14 (6th Cir. Dec. 14, 2010) (use of § 2703 process to obtain content of email messages).

discern a person's location. For example, traditional land-line telephone records reveal that a caller was using a particular land-line telephone number at a particular time, and investigators have long been able to use such information to place a caller in a particular location (often a private home) at the time of the call. However, telephone users have no reasonable expectation of privacy in this land-line information, even when collected in real-time, when the government obtains it from the phone provider. *See Smith*, 442 U.S. at 745 (concluding that phone user had no legitimate expectation of privacy in phone numbers he dialed); *Reporters Committee for Freedom of Press v. AT&T*, 593 F.2d 1030, 1046 n.49 (D.C. Cir. 1978) (citing cases for proposition that telephone subscribers have no Fourth Amendment basis for challenging government inspection of their toll records). In this respect, IP address connection records are no different than land-line telephone records, except that they are *less* geo-specific, not more, since many computers are considerably more mobile than land-line telephones. Further, the government is not required to obtain a warrant before compelling businesses to produce other types of business records from which location-based inferences could be drawn, such as bank records, employment records, credit card records, and other records of customer purchases. *See, e.g.*, *Miller*, 425 U.S. at 444 (rejecting Fourth Amendment challenge to subpoena for bank records). In short, the Subscribers do not have a Fourth Amendment interest in Twitter's records of their IP addresses even if the government could use these records to discern the Subscribers' locations at certain times.

The cases cited by the Subscribers do not support their claim that they have a Fourth Amendment interest in Twitter's IP address records. First, *United States v. Karo*, 468 U.S. 705 (1984), requires the government to obtain a warrant before using a tracking device to reveal

information about the interior of a private location. 468 U.S. at 715. But neither the Supreme Court nor the Fourth Circuit has applied this tracking-device standard to business records, even though many kinds of business records could reveal someone's location at a particular time. Indeed, if *Karo* did apply to business records, it would implicitly overrule *Smith v. Maryland*, *United States v. Miller*, and other Supreme Court cases that have upheld the government's ability to obtain business records without a warrant. Plainly, *Karo* did not void all of this settled precedent.

Furthermore, applying the *Karo* standard to all business records would have absurd and unworkable results. For example, the government would have to obtain a warrant, rather than a subpoena, to require a company to disclose phone records, security surveillance videos, visitor sign-in sheets, or even time-stamped photographs of an employee in her office, because any of these records could reveal someone's location in a private space at a particular time. *See United States v. Gray*, 491 F.3d 138, 153 (4th Cir. 2007) (citing *O'Connor v. Ortega*, 480 U.S. 709 (1987)) ("[A]n individual can have an expectation of privacy in his workplace."). The logical result of such an expansion of *Karo* would be that the government would be required to use a warrant, rather than a subpoena, whenever it sought to obtain business records. The Fourth Amendment has never been so construed.

Even if the *Karo* tracking-device standard were somehow applicable here, the Subscribers still would have no Fourth Amendment interest in Twitter's records of their IP addresses. Although the government must obtain a warrant to use a tracking device to "reveal a critical fact" about the interior of a private home, *Karo*, 468 U.S. at 715, no warrant is required when the government obtains more generalized information about a tracking device's location, even when

the device is actually located in a private space.[8] *See id.* at 720 (finding no Fourth Amendment violation when government used tracking device to determine that can of ether was inside warehouse because, *inter alia*, the device "did not identify the specific locker in which the ether was located"). Twitter's IP address records, without more, do not reveal the type of precise location information protected by the *Karo* standard. *See* (Mot. Vacate at 11 n.9 ("[O]ne of the leading companies advertises that its free geolocation tool can determine the location of '79% [of U.S. IP addresses] within a 25 mile radius.").) Accordingly, even if *Karo* applied to business records, the Subscribers have failed to establish that the government's acquisition of Twitter IP address records would violate a Fourth Amendment right under *Karo*. *Cf. United States v. Ortega-Estrada*, 2008 WL 4716949, at *13 (N.D. Ga. Oct. 22, 2008) (finding that even GPS information accurate to within 32 meters "revealed only a general area where the suspect was at a particular time, and thus, did not invade a place where he might have an expectation of privacy").

The *Third Circuit Opinion*, on which the Subscribers principally rely, also does not help their cause. (Mot. Vacate at 13.) In that case, the court agreed that the privacy interests at issue in *Karo* "are confined to the interior of the home," *Third Circuit Opinion*, 620 F.3d at 312, and it declined to hold that probable cause was always required for the government's collection of historical cell-site location information (CSLI) because there was no evidence in the record that

[8]The Subscribers cite a recent D.C. Circuit decision, *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), which suggests that the continued use of a tracking device in public may raise additional issues under the Fourth Amendment. (Mot. Vacate at 14.) In addition to being inapplicable here, this decision is inconsistent with Supreme Court precedent, including *Smith v. Maryland* and *Katz v. United States*, 389 U.S. 347 (1967), and conflicts with tracking-device decisions of three other courts of appeals. *See United States v. Marquez*, 605 F.3d 604, 609-10 (8th Cir. 2010); *United States v. Pineda-Moreno*, 591 F.3d 1212, 1216-17 (9th Cir. 2010); *United States v. Garcia*, 474 F.3d 994, 997-98 (7th Cir. 2007).

historical CSLI revealed information about the interior of a home.[9] *See id.* at 313. Likewise, the Subscribers have presented no evidence that Twitter's IP address records would reveal information about the interiors of their homes. Furthermore, even if the Third Circuit's opinion were persuasive and binding on this Court, *cf.* 620 F.3d at 320 (Tashima, J., concurring) (noting that majority opinion "vests magistrate judges with arbitrary and uncabined discretion to grant or deny issuance of § 2703(d) orders at the whim of the magistrate, even when the conditions of the statute are met" (footnote omitted)), its reasoning is inapplicable to the collection of IP addresses because such addresses are much more analogous to the phone numbers collected in *Smith v. Maryland* than they are to CSLI. Accordingly, even though the Third Circuit concluded that *Smith* is inapplicable to CSLI (a conclusion with which the government disagrees), it does not follow that *Smith* is inapplicable to IP address records.[10] In fact, just eight days after issuing the *Third Circuit Opinion*, the Third Circuit cited *Smith* in support of its conclusion that "no reasonable expectation of privacy exists in an IP address." *United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010).

In summary, for all of these reasons, the Order does not implicate the Subscribers' Fourth Amendment rights, and cannot be vacated on that ground.

D. Having Properly Issued the Order, This Court Need Not

[9]Records of CSLI reveal among other things the location of the antenna tower that carried a given call at a particular date and time. *See Third Circuit Opinion*, 620 F.3d at 308.

[10]The Third Circuit distinguished *Smith* on the ground that cell-phone customers do not "voluntarily" share CSLI with their phone providers. *See Third Circuit Opinion*, 620 F.3d at 317-18. This basis for distinguishing *Smith* is not available to the Subscribers because, as discussed above, they voluntarily conveyed their IP address information to Twitter when they logged into their Twitter accounts. Moreover, in an increasingly tech-savvy world, the notion, baldly asserted by the Subscribers, that a typical Internet user has no awareness that his IP address is transmitted to the Internet sites with which he or she communicates (such as Twitter), is dubious at best. (Mot. Vacate at 14.)

Reconsider Its Decision and Should Reject the Subscribers' Constitutional Avoidance Argument.

The Subscribers next ask the Court to apply the doctrine of constitutional avoidance in light of a § 2703(d) application that supposedly "raises serious constitutional questions," and to vacate the Order and require that the government instead obtain a warrant based on probable cause. (Mot. Vacate at 16.) But as demonstrated *supra*, although the Subscribers try gamely to conjure them, no "serious constitutional questions" attend the government's straightforward § 2703(d) application in this case. And even if, as Subscribers claim, § 2703(d) gave courts the discretion to "deny applications for § 2703(d) orders" that satisfy the § 2703(d) standard (Mot. Vacate at 14), that discretion would be inapplicable here, since the Court is not being asked to rule on a pending application, but instead to vacate its already-issued order. The Subscribers have identified no provision of the SCA that gives courts the discretion to vacate valid orders in order to avoid deciding constitutional challenges. Indeed, as detailed *supra* in Section II(A), the Subscribers are seeking yet another improvised remedy not authorized by the SCA. Accordingly, the Court should decline the Subscribers' invitation to vacate the Order.

Additionally, the alternative reading of § 2703(d) advanced by the Subscribers is contrary to the statute's language and structure. The Subscribers' argument relies on a Third Circuit case interpreting the "only if" language of § 2703(d) to mean that the "specific and articulable facts" requirement is a necessary condition for obtaining a 2703(d) order, but not a sufficient one. *See Third Circuit Opinion*, 620 F.3d at 319 (stating that § 2703(d) "gives the MJ the option to require a warrant showing probable cause," although such a requirement was "an option to be used sparingly"). This alternative interpretation of § 2703(d) should be rejected because it renders

superfluous the phrase "and shall issue" in § 2703(d). The Subscribers' "necessary but not necessarily sufficient" interpretation of § 2703(d) is equivalent to the following formulation, which omits the critical "and shall issue" language of § 2703(d): a § 2703(d) order "may be issued by any court that is a court of competent jurisdiction only if the governmental entity offers specific and articulable facts . . . ." The Subscribers' interpretation therefore violates the cardinal principle of statutory construction that a statute ought whenever possible be construed in such a way that no "clause, sentence, or word shall be superfluous, void, or insignificant." *Gunnells v. Healthplan Servs.*, 348 F.3d 417, 439-40 (4th Cir. 2003) (quoting *TRW Inc. v. Andrews*, 534 U.S. 19, 21 (2001) (internal quotation marks omitted)). Furthermore, the word "shall" has critical importance in a statute: "[t]he word 'shall' is ordinarily 'the language of command.'" *Alabama v. Bozeman*, 533 U.S. 146, 153 (2001). Because the Subscribers' interpretation of § 2703(d) improperly renders "shall" superfluous, it offers no basis for the Court's reconsideration of the Order.

Moreover, as Judge Tashima stated in his concurrence in *Third Circuit Opinion*, the Subscribers' construction of § 2703(d) "provides no standards for the approval or disapproval of an application" for a § 2703(d) order. 620 F.3d at 319 (Tashima, J., concurring). Their interpretation would permit a magistrate judge to arbitrarily deny an application under § 2703(d) without any reasoned basis. As Judge Tashima stated, such an interpretation "is contrary to the spirit of the statute." *Id.* The Subscribers divine a "sliding scale" at work in § 2703(d), Subscribers' Brief at 15, but fail to delimit how far the scale may slide: indeed, under the Subscribers' interpretation of the language of § 2703(d), a court could reject a § 2703(d) order even if the government established probable cause. In enacting the SCA, Congress could not

have intended such a chaotic and standard-less regime.

Furthermore, the Subscribers' argument that their interpretation of § 2703(d) is required by the doctrine of constitutional avoidance is mistaken. Under this doctrine, "when an Act of Congress raises a serious doubt as to its constitutionality, [courts should] first ascertain whether a construction of the statute is fairly possible by which the question may be avoided." *Zadvydas v. Davis*, 533 U.S. 678, 689 (2001) (internal citations omitted). Here, as shown *supra*, the Subscribers have utterly failed to raise serious doubts about the constitutionality of § 2703(d), rendering that doctrine inapposite.

Thus, there is no reason for this Court to avoid any constitutional challenges, serious or otherwise, raised by the Subscribers. "[I]n a field like search and seizure law, where lawmakers are continually struggling to update legislation to cope with changing technology, the presumption, inherent in the doctrine of constitutional avoidance, that Congress did not intend to promulgate legislation which 'raises serious constitutional doubts,' has little applicability." *In re Application of the United States*, 632 F. Supp. 2d 202, 210 (E.D.N.Y. 2008) (internal citation omitted). For all of these reasons, the Court should reject the Subscribers' constitutional avoidance argument and decline to vacate the Order.

E. Subscriber Jonsdottir's Status as a Member of Iceland's Parliament Does Not Insulate Twitter's Records From Disclosure Under the Order.

Lastly, the Subscribers claim that Ms. Jonsdottir's status as a member of the Icelandic Parliament means that the Order "appears to violate Icelandic law," since she is "protected by a strong constitutional immunity in Iceland." (Mot. Vacate at 16.) The Subscribers protest that the government "is conducting a criminal investigation which sweeps in Ms. Jonsdottir's

publications in Icelandic on topics of Icelandic concern – records that could not be obtained under Icelandic law." (Mot. Vacate at 16-17.) The Subscribers also darkly warn that this investigation "creates a perilous precedent for foreign government efforts to seek information about members of the U.S. Congress," and urge that the Order be vacated. (Mot. Vacate at 17.)

In raising their legislative immunity claim, the Subscribers invoke the Speech or Debate Clause. (Mot. Vacate at 16 n.12). It provides, "for any Speech or Debate in either House, [Senators and Representatives] shall not be questioned in any other place." U.S. Const. art. I, § 6, cl. 1. The Speech or Debate Clause "serves to immunize a member of Congress from being questioned about his legislative acts." *United States v. Jefferson*, 546 F.3d 300, 304 n.2 (4th Cir. 2008). "Put simply, the Clause provides legislators with absolute immunity for their legislative activities, relieving them from defending those actions in court." *Id.* at 310. But the constitutional protections afforded legislators are limited and circumscribed. The Speech or Debate Clause prohibits "inquiry only into those things generally said or done in the House or the Senate in the performance of official duties and into the motivation for those acts." *United States v. Brewster*, 408 U.S. 501, 512 (1972); *United States v. Jefferson*, 534 F. Supp. 2d 645, 651 (E.D. Va. 2008) ("[T]he privilege applies only to those activities integral to a Member's legislative function, *i.e.*, activities that are integral to the Member's participation in the drafting, consideration, debate, and passage or defeat of legislation" (footnotes omitted)). But the Clause does not bar an "inquiry into activities that are casually or incidentally related to legislative affairs but not a part of the legislative process itself." *Brewster*, 408 U.S. at 528. And, of course, "the Speech or Debate Clause is not a license to commit crime." *Jefferson*, 534 F. Supp. 2d at 652.

Here, the Subscribers' assertion of legislative immunity based on Ms. Jonsdottir's status as a foreign legislator is fatally flawed, in several respects. First, of course, Ms. Jonsdottir is not a member of Congress, and thus cannot claim the protections of the Speech or Debate Clause. That Clause by its terms applies only to "Senators and Representatives." *See United States v. Gillock*, 445 U.S. 360, 366 n.5 (1980).

Second, even if apart from the Speech or Debate Clause Ms. Jonsdottir qualifies for "legislative immunity" in courts of the United States, *see E.E.O.C. v. Wash. Suburban Sanitary Comm.*, — F.3d —, 2011 WL 228591 (4th Cir. 2011) (protected legislative acts "generally bear the outward marks of public decisionmaking, including the observance of formal legislative procedures"), in this preliminary investigative proceeding there is no occasion to assert that doctrine. The Order seeks business records from Twitter, not Ms. Jonsdottir. It does not require Ms. Jonsdottir's participation or presence, or that she do anything at all. The Order does not seek sensitive or confidential information, but rather data that Ms. Jonsdottir voluntarily provided to an American corporation, and in which she has no privacy interest. The Order does not compel testimony - from any person. *Cf.* U.S. Const. art. I, § 6, cl. 1 (legislators "shall not be questioned . . . ."). It does not seek content - so it is irrelevant whether Ms. Jonsdottir's Tweets were "predominantly in Icelandic," or in any other language. (Mot. Vacate at 16.) It does not seek information about any aspect of parliamentary affairs in Iceland, including any of Ms. Jonsdottir's legislative acts or activities. It does not seek information regarding other Twitter accounts known to be used by members of Iceland's parliament; the other Subscribers do not hold such status. In short, upon examination, the Subscribers' claim that Ms. Jonsdottir's status as a parliamentarian gives rise to "concerns" in this § 2703(d) proceeding is vacuous. *Cf. Wash.*

Suburban Sanitary Comm., 2011 WL 228591, at *9 (refusing to quash administrative subpoena at preliminary stage of investigation where it was unknown whether investigation would evolve into lawsuit or whether defending such a suit would require legislators' testimony or involvement).

Third, even if Ms. Jonsdottir could invoke legislative immunity here, and further could show that she used her Twitter account to communicate with her constituents about matters in Iceland's parliament, that factor is of no moment, since her Tweets to constituents were not protected legislative acts. The Founders never intended to grant legislative immunity "for defamatory statements scattered far and wide by mail, press, and the electronic media." *Hutchinson v. Proxmire*, 443 U.S. 111, 132 (1979). Moreover, a legislator's public statements, including newsletters and press releases, are "not part of the legislative function or the deliberations that make up the legislative process." *Id.* at 133. Accordingly, "transmittal of such information by press releases and newsletters is not protected by the Speech or Debate Clause." *Id.* It follows that the Subscribers cannot hope to demonstrate that Ms. Jonsdottir is entitled to legislative immunity - whatever that might mean in this § 2703(d) proceeding - based on her public Tweets.

Fourth, and finally, a legislator cannot decline to participate in a lawful criminal investigation, or prevent others from doing so, based on his or her status. In *Gravel v. United States*, 408 U.S. 606 (1972), a United States Senator moved to quash a federal grand jury subpoena served on a member of the senator's own staff. The grand jury was investigating possible crimes relating to the release and dissemination of the Pentagon Papers. It appeared that the Senator had read extensively to a subcommittee from the Pentagon Papers (which were then

classified) and had placed all 47 volumes in the public record, and had afterwards negotiated with publishers about publishing the documents. 408 U.S. at 609-10. In the grand jury investigation, the Senator intervened, citing the Speech or Debate Clause, and moved to quash the subpoena and to require the government to specify the questions to be asked his aide.

The Supreme Court held that the Senator's aide was required to testify before the grand jury. Reflecting upon the Speech or Debate Clause, the Court stated:

> [The Clause], as we have emphasized, does not purport to confer a general exemption upon Members of Congress from liability or process in criminal cases. Quite the contrary is true. While the Speech or Debate Clause recognizes speech, voting, and other legislative acts as exempt from liability that might otherwise attach, it does not privilege either Senator or aide to violate an otherwise criminal law in preparing for or implementing legislative acts. If republication of these classified papers would be a crime under an Act of Congress, it would not be entitled to immunity under the Speech or Debate Clause. It also appears that the grand jury was pursuing this very subject in the normal course of a valid investigation.

408 U.S. at 626. The Court further opined that it did not "perceive any constitutional or other privilege that shields [the aide], any more than any other witness, from grand jury questions relevant to tracing the source of obviously highly classified documents that came into the Senator's possession and are the basic subject of inquiry in this case, as long as no legislative act is implicated by the questions." *Id.* at 628 (footnote omitted).

Gravel demonstrates that a senator cannot use his status to exempt himself from a criminal investigation, or to prevent a third party from complying with lawful investigative process. *See Brewster*, 408 U.S. at 516 (purpose of Speech or Debate Clause was not "to make Members of Congress super-citizens, immune from criminal responsibility"). Here, Ms. Jonsdottir manifestly cannot invoke her position as an Icelandic parliamentarian and thereby

block Twitter's compliance with an Order to provide non-privileged and non-content information that she voluntarily relinquished to that corporation months ago. Even if she were a member of Congress, she could not do so.

III. *Conclusion*

For the reasons stated, this Court should deny the Subscribers' motion to vacate the Order of December 14, 2010.

Respectfully submitted,

Neil H. MacBride
United States Attorney

By: /s/
John S. Davis
Tracy Doherty-McCormick
Assistant United States Attorneys
United States Attorney's Office
2100 Jamieson Avenue
Alexandria, Virginia 22314
(703) 299-3700

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a true copy of the foregoing Objection was filed with the Clerk of the Court on February 7, 2011, and a copy of this filing was e-mailed to opposing counsel at the following addresses:

John K. Zwerling
Stuart Sears
Zwerling, Liebig & Moseley, P.C.
108 N. Alfred Street
Alexandria, VA 22314
JZ@Zwerling.com
Counsel for Jacob Appelbaum

Johnathan Shapiro
Greenspun, Shapiro, Davis, & Leary
3955 Chain Bridge Rd
Second Floor
Fairfax, VA 22030
Js@greenspunlaw.com
Counsel for Birgitta Jonsdottir

Nina J. Ginsberg
Dimuro Ginsberg P.C.
908 King Street, Suite 200
Alexandria, VA 22314
nginsberg@dimuro.com
Counsel for Rop Gonggrijp

Rebecca K. Glenberg
ACLU of Virginia Foundation, Inc.
530 E. Main Street, Suite 310
Richmond, VA 23219
rglenberg@acluva.org

/s/
John S. Davis
Assistant United States Attorney
2100 Jamison Avenue
Alexandria, VA 22314
Phone: (703) 299-3700
Fax: (703) 299-3982

ATTACHMENT I

THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE 2703(d) ORDER AND 2703(f) PRESERVATION REQUEST RELATING TO GMAIL ACCOUNT	Case No. 1:10GJ3793 11-DM-2 **UNDER SEAL**

RESPONSE OF THE UNITED STATES TO GOOGLE'S MOTION TO STAY PRODUCTION PENDING RULING ON GOOGLE'S OBJECTION TO MAGISTRATE'S ORDER

The United States, by and through Neil H. MacBride, United States Attorney, opposes Google Inc.'s ("Google") motion to stay production of documents ("Google Motion to Stay") pending this Court's ruling on Google's motion objecting to ("Google Motion") Magistrate Judge [redacted] decisions that the court-ordered legal process for business records pursuant to the Stored Communications Act ("SCA") (18 U.S.C. §§ 2701-12) should remain under seal and not be disclosed for a limited period of time pending the ongoing criminal investigation.

As further described in the factual background of the Government's Response to Google's Motion ("Government Response"), incorporated here by reference, Google has objected to Magistrate [redacted] ruling on February 9, 2011 that denied in part and granted in part Google's motion to modify the court's order of January 4, 2011 (the "Order") requiring Google to produce subscriber and transaction records related to the Gmail account [redacted] (the "[redacted] subscriber") under 18 U.S.C. § 2703(d). Google had asked Judge [redacted] to unseal and vacate the Order's non-disclosure provisions, which the court had properly included pursuant to 18 U.S.C. § 2705 and Local Criminal Rule 49, so that Google could "provide *immediate* notice" to the ioerror subscriber. Google Mot. at 2 (emphasis added). Magistrate

[redacted] adopted, instead, the government's reasonable proposal to modify the Order to authorize Google to provide notice to the [redacted] subscriber "within (90) days of providing . . . the information requested in [the] Order, unless the government files a motion for an extension of that non-notification period." Roche Decl. Ex. 4. Magistrate Davis further ordered "that the government may request an extension of the [Order's] non-notification period for a maximum of sixty (60) days." ("Order 2") *Id.*

For the reasons set forth below, the United States opposes Google's Motion to Stay its production of documents and information pending the court's consideration of its objections. Google has failed to meet its burden to show that this Court should exercise its discretion and grant a stay. It failed to show a strong likelihood of success on the merits and irreparable injury absent a stay. To the contrary, a stay will injure the United States and is contrary to the public's interest.

Standard of Review

In deciding whether to stay enforcement of an order, the Court should consider the following factors: "(1) whether the stay applicant has made a strong showing that he is likely to succeed on the merits; (2) whether the applicant will be irreparably injured absent a stay; (3) whether issuance of the stay will substantially injure the other parties interested in the proceeding; and (4) whe[re] the public interest lies." *GTSI Corp. v. Wildflower Int'l, Inc.*, No. 1:09cv123, 2009 WL 3245396 at *1 (E.D.Va. Sept. 29, 2009) (citing *Hilton v. Braunskill*, 481 U.S. 770, 776 (1987) (collecting cases) and James Wm. Moore, *Moore's Federal Practice* § 62.06[3] (3d ed.2007)); *United States v. Clark*, Nos. C-79-190-G, 193G, 1980 WL 1502 at *1 (M.D.N.C. Feb. 6, 1980) (citing 11 Wright & Miller, *Federal Practice and Procedure* § 2904 at

316 (1973) and *Long v. Robinson*, 432 F. 2d 977 (4th Cir. 1970)); *see also United States v. Dyer*, 750 F.Supp. 1278, 1299 n. 40 (E.D.Va. 1990).

"A stay is not a matter of right, even if irreparable injury might otherwise result." *Nken v. Holder*, 129 S.Ct. 1749, 1760-61 (2009) (quoting *Virginia R. Co., v. United States*, 272 U.S. 658, 672 (1926)). It is "an exercise of judicial discretion," and its issuance depends "upon the circumstances of the particular case." *Nken*, 129 S.Ct. at 1761 (citing *Virginia R. Co*, 272 U.S. at 672-673 and *Hilton*, 481 U.S. at 777). The party seeking a stay bears the burden to show "that the circumstances justify an exercise of that discretion." *Nken*, 129 S.Ct. at 1761 (citing *Clinton v. Jones*, 520 U.S. 681, 708 (1997); *Landis v. North American Co.*, 299 U.S. 248, 255 (1936)).

Analysis

I. Google Has Failed to Make a Strong Showing that It is Likely to Succeed on the Merits

The Court must consider the following two aspects in weighing Google's likelihood of success: (1) the standard of review used to determine whether to overturn Magistrate [redacted] determination of a non-dispositive motion; and (2) the underlying merits. *GTSI Corp.*, 2009 WL 3245396 at *1.

A. Standard of Review

The parties disagree on the appropriate standard of review. *See* Google Mot. at 8; Gov't Resp. at 4-6. The United States believes that Google's motion involves non-dispositive matters under Rule 59(a) of the Federal Rules of Criminal Procedure. *See In re U.S. for Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, Mag. No. 07-524M, 2008 WL 4191511, at *1 (W.D. Pa. Sept. 10, 2008), *vacated on other grounds by* 620 F.3d 304 (3d Cir. 2010) (reviewing objections to magistrate judge's denial of a § 2703(d) court order under Fed. R. Crim. P. 59(a) and 28 U.S.C. § 636(b)(1)); *In re U.S. for an Order*

Authorizing the Disclosure of Prospective Cell Site Information, No. 06-MISC-004, 2006 WL 2871743, at *1 (E.D. Wisc. Oct. 6, 2006) (same).

Non-dispositive orders are overturned only if "clearly erroneous or contrary to law." *See* Fed.R.Crim.P. 59(a); *see also* 28 U.S.C. § 636(b)(1)(A) ("A judge of the court may reconsider any pretrial matter under this subparagraph (A) where it has been shown that the magistrate judge's order is clearly erroneous or contrary to law."); *GTSI Corp.*, 2009 WL 3245896 at *2 (district court should overturn magistrate judge's civil discovery order only if it is "clearly erroneous or contrary to law").

Google argues for a de novo standard of review on the basis that the Orders are dispositive as to Google, a third-party recipient of court-ordered process. Google is wrong as demonstrated by the plain reading of Rule 59 of the Federal Rules of Criminal Procedure.[1] Further, the cases Google cites in support of *de novo* review are inapposite, applying to whether a district court order is an immediately appealable final order for purposes of appellate review under 28 U.S.C. § 1291, not to whether a Magistrate's Order is dispositive or non-dispositive under Rule 59.

Therefore, the appropriate standard of review is the standard set forth in Rule 59(a), clearly erroneous or contrary to law. In any event, even were the court to conduct a de novo review, Judge [redacted] Orders are correct, not contrary to law. No error was committed, let alone clear error.

[1] Rule 59(a) authorizes a party to file objections to a magistrate judge order that determines "any matter that does not dispose of a charge or defense," Fed. R. Crim. P. 59(a), while Rule 59(b) authorizes a party to file objections to a magistrate judge's "proposed findings and recommendations" for disposing of "a defendant's motion to dismiss or quash an indictment or information, a motion to suppress evidence, or any matter that may dispose of a charge or defense." Fed. R. Crim. P. 59(b)(1), (2).

B. Merits of Google's Objections

Google objects to the Orders principally because it wishes to immediately disclose the existence of the Order to the [redacted] subscriber *before* producing the required records instead of waiting 90 days *following* its production to make the disclosure. Thus, Google disagrees with Magistrate Judge [redacted] decision to include non-disclosure and sealing provisions in the Order.

As discussed in the Government's Response, however, Judge [redacted] has already limited the duration of the non-disclosure and sealing provisions, and Google has failed to demonstrate that Magistrate [redacted]' order of such provisions was unlawful or erroneous in any respect. Gov't Resp. at 10-11. Google has failed to articulate (1) how compliance with the non-disclosure and sealing provisions unduly burdened Google under § 2703(d)[2] and (2) any other statutory provision authorizing Google to challenge such provisions. *Id.*

Google's Motion does not even discuss this issue except for proffering its opinion that there is no need for secrecy. Google Mot. at 9-12. The Government's Response refutes this opinion, amply demonstrating that: (1) the non-disclosure and sealing provisions in the Order remain valid and warranted more than ever (Gov't Response at 8-10); and (2) the unsealing and disclosure of the Twitter Order has already seriously jeopardized the investigation, and additional disclosures will exacerbate the harm caused by that disclosure. Gov't Resp. at 16-18.

It is not enough that Google's "chance of success on the merits be 'better than negligible.'" *Nken,* 129 S.Ct. at 1761 (quoting *Sofinet v. INS,* 188 F.3d 703, 707 (7th Cir. 1999). Google must make a "strong showing," *GTSI Corp.* 2009 WL 3245396, at *1, that it is likely to succeed. It has not made such a showing. Google has failed to show that Judge [redacted]

[2] Pursuant to this section, a service provider, such as Google, may move to quash or modify an 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).

conclusions were erroneous, and it has certainly not shown that they were clearly erroneous or contrary to law. Gov't Resp. at 10-11. Google is not likely to succeed on the merits of its objections, and its motion to stay should fail for this reason alone.

Google, however, persists in claiming that the non-disclosure and sealing provisions may prevent the [redacted] subscriber from raising constitutional issues and that such provisions constitute an unconstitutional prior restraint on Google's free speech. Google Mot. at 11-12. To the contrary, as is more fully described in the Government's Response, at 11-16, Google has failed to show -- and has not even come close to establishing a "strong" showing -- that it is likely to succeed on these claims. The Orders satisfy all statutory and constitutional requirements, and the sealing and non-disclosure provisions, which are now of limited duration, should remain in effect. Google has established no statutory basis for it to challenge the Order and has no meritorious First Amendment challenge to a 90-day non-disclosure provision (with the potential for 60 additional days), pending the ongoing investigation. *Id.* The [redacted] subscriber is not entitled to notice under § 2703(d), and the [redacted] subscriber would not have a valid basis to challenge the Order even if Google did provide him with notice. *Id.*

II. Google Has Failed to Show that it will be Irreparably Injured Absent a Stay

Google has failed to show how *its* rights will be injured by producing the required records pending a court decision on the delayed disclosure provisions of the Order. Although Google alludes to possible injury of its First Amendment rights, this misses the mark. Google seeks to stay its production of records from the [redacted] subscriber account – not to stay the non-disclosure and sealing provisions. And, Google has wholly failed to explain how production of such records implicates its First Amendment interests whatsoever. In other words, pending this Court's decision on Google's objections, the non-disclosure and sealing provisions of the Order

apply to Google. In the meantime, Google cannot disclose the Order's existence irrespective of the outcome. Thus, granting or denying Google's motion to stay the production of records is irrelevant to Google's alleged First Amendment rights to disclosure. Denying the stay does not irreparably injure any such right, even assuming such a right exists.

Google attempts to overcome its lack of injury by linking itself to alleged injuries that it speculates the [redacted] subscriber might suffer. Thus, Google's Motion to Stay primarily rests on the claim that once Google produces the records, the Court cannot "unring the bell." Google Mot. to Stay at 4-5 (citing *Maness v. Meyers*, 419 U.S. 449, 460 (1975)). Even assuming Google can properly step into the shoes of the [redacted] subscriber, its conclusory statements insufficiently establish irreparable injury. The Order does not prevent Google from notifying the [redacted] subscriber forever. It simply delays notification until after Google has produced the documents for a reasonable period of time pending the ongoing criminal investigation. Google presumably will notify the [redacted] subscriber at the appropriate time after the records have been produced. The subscriber remains free, at that time, to attempt to challenge the disclosure or wait to challenge any use of such records in court. Google has not asserted that the production of the relevant records would waive any privilege or claim that the [redacted] subscriber might have. Even if there were such a claim or privilege, the subscriber would not suffer "irreparable injury" because he could adjudicate any such claims at another stage in the proceedings. *See generally, New York Times Co. v. Jascalevich*, 439 U.S. 1301, 1302 (1978) (denying application for stay of New Jersey Supreme Court order that refused to stay and denied leave to appeal an order of a state trial court refusing to quash a subpoena to New York Times and reporter issued in a criminal trial: applicants would have a full hearing and there was no authority that a newsman need not produce material documents; the Court would prefer to address any issues at a later

stage in the proceedings, and because the trial court viewed the documents sufficiently material to conduct an *in camera* inspection, no perceptible irreparable injury); *Mohawk Industries Inc. v. Carpenter,* --- U.S. ----, 130 S.Ct. 599, 607 (2009) (in ruling that a disclosure order of attorney-client privilege documents did not qualify for immediate appeal, explaining that [a]ppellate courts can remedy the improper disclosure of privileged material in the same way they remedy a host of other erroneous evidentiary rulings: by vacating an adverse judgment and remanding for a new trial in which the protected material and its fruits are excluded from evidence."); *United States v. Myers,* 593 F.3d 338, 346 (4th Cir. 2010).

III. The Issuance of a Stay will Substantially Injure the United States

Google argues that the government will suffer no harm if the Court grants the motion to stay production of the subscriber and transactional records from the [redacted] account. Google claims that there is no risk that the records will be destroyed, so the only issue is when the government will receive the records. Google Mot. to Stay at 5.

To the contrary, Google's resistance to providing the records has already frustrated the government's ability to efficiently conduct a lawful criminal investigation. The Order was issued by a neutral magistrate judge on January 4, 2011. Google's compliance was due within three days thereafter. The two-month delay in getting the sought-after records has already prejudiced the investigation. *See Nken,* 129 S.Ct. at 1757 ("[t]he parties and the public, while entitled to both careful review and a meaningful decision, are also generally entitled to the prompt execution of orders that the legislature has made final."). First, the delay has deprived the government of potential evidence. Second, the delay has prevented the government from sending follow-up legal process, as needed, on investigative leads from the records. For instance, the records might identify accounts or other subscriber information of which the

government is unaware or might include transactional information helpful to obtain search warrant(s).

Google's attempt to stay production of routine legal process based on its unfounded objections to the non-disclosure and sealing provisions of the Order have diverted time and attention from the investigation. Google attempts to escape this by claiming the government is not harmed because it agreed to a stay on the Twitter matter and moved to continue Magistrate [redacted] hearing until Judge [redacted] could rule on the underlying merits of the Twitter subscribers' claims.[3] That is not the legal standard. The harms suffered by the government are synonymous with the public's interest in effective law enforcement and the efficient conduct of the criminal justice system. Indeed, "these [two] factors merge when the Government is the opposing party." *Nken*, 129 S.Ct. at 1762. The public's interest is addressed further below.

IV. The Public's Interest in Law Enforcement and the Effective and Efficient Administration of the Criminal Justice System is Best Served by Requiring Google to Disclose the Records Pending the Court's Consideration of its Objections

Google focuses on whether the public interest is served by its *disclosure of the Order to the [redacted] subscriber*. Google Mot. to Stay at 5-6 ("the public can have no interest in the enforcement of a nondisclosure provision" where the investigation is public). Again, this is not at issue in the instant motion. The issue presented here is whether a stay on Google's *production of the required records* serves the public interest. It does not. Conversely, the public interest in effective law enforcement and the efficient administration of the criminal just system has been firmly established in a variety of contexts. *See generally, e.g., Zurcher v. Stanford Daily*, 436 U.S. 547, 560-62 n. 8 (1970) (recognizing the fundamental public interest in implementing the

[3] The government made this motion on the basis of Google's concern that a decision by Magistrate [redacted] would "prejudge[] any free speech or privilege objections that Google's user may wish to raise by describing them as meritless." *See* Gov't Motion to Continue Hearing at 1.

and effective administration of the criminal justice system will be harmed by a stay. Thus, the Court should deny Google's Motion to Stay.

Respectfully Submitted,

[redacted]
United States Attorney

By: [redacted]
Assistant United States Attorney

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing pleading was delivered on this 28th day of February 2011 to the Clerk's Office and that service will be made on the following individuals by electronic mail and otherwise:

John K. Roche, Esquire
Perkins Coie LLP
700 13th St., N.W., Suite 600
Washington, D.C. 20005-3960
PHONE: 202.434.1627
FAX: 202.654.9106
E-MAIL: JRoche@perkinscoie.com

[redacted]
Assistant United States Attorney

ATTACHMENT J

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

IN RE 2703(d) ORDER AND 2703(f) PRESERVATION REQUEST RELATING TO GMAIL ACCOUNT [redacted]	Misc. No. 10GJ3793 11-DM-2 FILED UNDER SEAL

GOOGLE INC.'S REPLY IN SUPPORT OF ITS OBJECTIONS TO MAGISTRATE'S ORDER OF FEBRUARY 9, 2011 AND NOTICE OF APPEAL PURSUANT TO FED. R. CRIM. P. 59

Google Inc. ("Google") hereby submits this Reply in Support of its Objections to Magistrate's Order of February 9, 2011 and Notice of Appeal Pursuant to Fed. R. Crim. P. 59.

The government has admitted that the demand at issue here (the "Order")[1] and the unsealed Twitter Order[2] relate to the same investigation. The government has also acknowledged that the subjects of the Twitter Order (including Twitter user [redacted] and anyone who has heard about the highly publicized Twitter Order) already are operating under the assumption that the government has sought information related to their Google accounts. These facts alone demonstrate that there is no cause for the Order to have been sealed in the first place or to remain sealed now. The government has "buyer's remorse" for having unsealed the Twitter Order, and wants Google's subscriber and Google to pay for the government's perceived mistake by compelled silence.

Rather than demonstrating how unsealing the Order to Google will harm its well-publicized investigation, the government lists a "parade of horribles" that allegedly have already

[1] *See* Declaration of John K. Roche, Ex. 1 ("Roche Decl.") (filed Feb. 17, 2011).

[2] *Id.* Ex. 2.

occurred since it unsealed the Twitter Order. The government fails to establish how any of these past developments could be further exacerbated by unsealing this Order. The subject of the Order likely already knows or has surmised that the government has sought the account information. All that compelled silence would accomplish here is to prevent the user from raising more informed objections and obtaining judicial review as the Twitter user [redacted] has sought to do in regard to the Twitter Order.

Accordingly, for these reasons and those stated below and in Google's Objections, Google respectfully requests that the Court modify the Order pursuant to the terms of Google's proposed order.

I. ARGUMENT

A. The Court's Standard of Review is *De Novo*

Judicial orders based on sealed certifications from the government must be reviewed *de novo* because review of such orders is done "*ex parte* and thus unaided by the adversarial process." *U.S. v. Rosen*, 447 F. Supp. 2d 538, 545 (E.D. Va. 2006) (rejecting the government's contention that a reviewing district court must accord the Foreign Intelligence Surveillance Court's probable cause determination "substantial deference"). Neither the government nor Judge [redacted] revealed anything to Google about what was included in the government's *ex parte* application for the Order, thus precluding any adversarial proceeding over the substance of that application. As such, respectfully, the Court owes no deference to Judge [redacted] conclusion that notification of the Order will "seriously jeopardiz[e] an investigation" under 18 U.S.C. § 2705. *Id.* (conducting *de novo* review "with no deference accorded to the [Foreign Intelligence Surveillance Court's] probable cause determinations").

Furthermore, as Google noted in its Objections, the Supreme Court and the Fourth Circuit have found that discovery orders directed at third parties are dispositive for appellate purposes. *U.S. v. Myers*, 593 F.3d 338, 345 (4th Cir. 2010) (discovery order directed at a third party is "an immediately appealable final order.") (quoting *Church of Scientology of California v. U.S.*, 506 U.S. 9, 18 n.11 (1992)). Accordingly, such orders are necessarily governed by the *de novo* standard of review for dispositive orders under Fed. R. Crim. P. 59(b)(3). The government claims these cases are inapposite because they address appeals from the decision of a district court to an appellate circuit court under 28 U.S.C. § 1291, rather than appeals from a magistrate judge to a district court judge under Fed. R. Cr. P. 59. *See* Government Response, at 7. This argument elevates form over substance because a district court acts in an appellate capacity when reviewing a magistrate's order, thus making these cases relevant to the Court's analysis.

B. Google Has a Right to Challenge the Nondisclosure Provision in the Order

The government erroneously claims that Judge [redacted] "concluded that Google has no statutory basis to challenge the non-disclosure and sealing provisions in the Order." *See* Government Response, at 10. In fact, Judge Davis partially granted Google's motion by limiting the nondisclosure period in the Order to 90 days, which he certainly would not have done had he concluded that Google had no right to bring the motion in the first place.

Furthermore, 18 U.S.C. § 2703(d) gives providers the right to ask a court to quash or modify an order when compliance "would cause an undue burden on such provider." This right must include the ability to challenge a provision in a § 2703(d) order that a provider believes is not adequately supported by fact or law. Were it otherwise, providers would be forced to blindly produce records even if they received an order that did not make any of the requisite findings under § 2703(d). *See* 18 U.S.C. § 2703(d) (requiring "specific and articulable facts showing that

there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation."). The government's interpretation of § 2703(d) must be rejected so as to avoid this absurd result. *Aremu v. Dep't of Homeland Security*, 450 F.3d 578, 583 (4th Cir. 2006) ("[A] court must, if possible, interpret statutes to avoid absurd results.").

C. The Government Cannot Show a Need for Secrecy of the Order or the Preservation Request

Regardless of what standard of review the Court applies, the government cannot satisfy the standard set forth in 18 U.S.C. § 2705(b)(5), which provides for nondisclosure when notification will result in "seriously jeopardizing an investigation."

First, the government attempts to justify the nondisclosure provision by claiming that unsealing this Order may cause the targets to "alter their modes of communication to evade future investigative efforts." *See* Government Response, at 17. However, the government has already conceded that the targets of the investigation are already working under the assumption that their Google accounts are the subject of legal process from this grand jury investigation. *See* Government Response (dated January 28, 2011), at 14; *see also* Government Exhibits 3-4.[3] Therefore, disclosing this Order will do nothing to alter anyone's behavior, except that [redacted] may exercise the right to defend his or her legal interests in court. And of course, to the extent [redacted] has already destroyed evidence, unsealing the Order will not reverse those actions either.

Second, the government rehashes its claim that unsealing the Order may result in "witness intimidation" in the form of encouraging providers "to feel pressure to challenge non-disclosure orders." *See* Government Response, at 18. This argument is specious for the reasons

[3] Roche Decl., Ex. 7; *see also* [redacted] retweet of Jan. 7, 2011 @ 9:26 p.m. ("Note that we can assume Google & Facebook also have secret US government subpoenas. They make no comment. Did they fold?"), http://twitter.com/[redacted] last visited Jan. 18, 2011).

previously noted in Google's Objections. Google will only add that if a provider believes a nondisclosure provision in an order is unlawful, then it *should* challenge the order. The government confuses witness intimidation with a provider's legitimate right to protect its First Amendment rights and the privacy of its users.

Finally, the government claims that its employees were harassed after the disclosure of the Twitter Order and that the same can be expected if this Order is disclosed. *See* Government Response, at 18. No public servant deserves such treatment, and in order to avoid any such incidents in the future, the government should request that the Court order any personal identifiers of government personnel redacted before unsealing the Order or preservation letter. Google would certainly agree that such a measure is appropriate here.

D. The Order May Raise Significant Constitutional and Statutory Issues

As Google noted in its Objections, three of the users identified in the Twitter Order, including Twitter's [redacted] user, filed a motion to vacate that order on Constitutional and statutory grounds.[4] That motion was argued on February 15th, and as of this writing is still under advisement before Judge [redacted]. One can only assume that if the users' arguments were as meritless as the government claims,[5] Judge [redacted] would have disposed of them from the bench, or without entertaining any oral argument at all, rather than considering them as Her Honor has for the better part of a month. And one can only surmise whether knowledge of the Order here would affect the users' claims or Judge [redacted]s decision-making. The gag order here serves the purpose only of preventing the user from fully articulating objections based on the full scope of the information sought.

---

[4] Roche Decl., Ex. 3.

[5] Government's Response, at 13.

E. The Order is a Prior Restraint on Google's Right to Free Speech

The government cannot seriously dispute the fact that the non-disclosure provision in the Order is a prior restraint on Google's First Amendment rights. *In re Sealing and Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 882 (S.D. Tex. 2008) ("a non-disclosure order imposes a prior restraint on speech."). The only question is whether the government can carry its "heavy burden of showing justification for the imposition of such a restraint." *Id.* (quoting *Capital Cities Media, Inc. v. Toole*, 463 U.S. 1303, 1305 (1983).

Google respectfully submits that because the government's interest in [redacted] electronic communications is already so well-publicized and there is absolutely no risk of destruction of evidence, the balance tips decidedly in favor of Google's First Amendment rights.

II. CONCLUSION

For the reasons stated here and in Google's Objections, Google respectfully requests that the Court sustain its Objections and modify the Order pursuant to the terms of Google's proposed order.

DATED this 7th day of March, 2011.

Respectfully submitted,

By _____

John K. Roche (VSB# 68594)
Perkins Coie LLP
700 13th St., N.W., Suite 600
Washington, D.C. 20005-3960
Phone: 202-434-1627
Fax: 202-654-9106
JRoche@perkinscoie.com

Albert Gidari (*admitted pro hac vice*)
Perkins Coie LLP

1201 Third Avenue, Suite 4800
Seattle, Washington 98101
Phone: 206-359-8000
Fax: 206-359-9000
AGidari@perkinscoie.com

Attorneys for Google Inc.

CERTIFICATE OF SERVICE

I hereby certify that on this 7th day of March, 2011, the foregoing document was sent via hand delivery and email to the following persons:

[redacted]
Assistant United States Attorney
United States Attorney's Office
Eastern District of Virginia
Justin W. Williams United States Attorney's Building
2100 Jamieson Avenue
Alexandria, VA 22314-5794
[redacted]

Attorneys for the United States

By _____
John K. Roche (VSB# 68594)
Perkins Coie, LLP
700 13th St., N.W., Suite 600
Washington, D.C. 20005-3960
Phone: 202-434-1627
Fax: 202-654-9106
JRoche@perkinscoie.com

Attorneys for Google Inc.

ATTACHMENT K

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

FILED

2011 MAR -7 P 12:07

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

IN RE 2703(d) ORDER AND 2703(f) PRESERVATION REQUEST RELATING TO GMAIL ACCOUNT [redacted]	Misc. No. 10GJ3793 11-DM-2 FILED UNDER SEAL

GOOGLE INC.'S REPLY IN SUPPORT OF ITS MOTION TO STAY PRODUCTION PENDING APPEAL OF MAGISTRATE'S ORDER

Google Inc. ("Google") hereby submits this Reply in Support of its Motion to Stay Production Pending Appeal of Magistrate's Order.

Google respectfully submits that a stay should be granted because, as demonstrated in its Objections and Reply in support thereof, it has made a strong showing of likely success on the merits. Furthermore, Google's subscriber and Google will suffer irreparable injury absent a stay because without a stay the very injury that Google seeks to avoid – production of documents and information without notice to its subscriber – will occur. Moreover, the issuance of a stay will not injure the government or harm the public interest, as illustrated by the fact that the government previously sought to continue Google's original motion to modify this Court's order of January 4, 2011 (the "Order")[1] until after Judge [redacted] resolved a similar motion related to the Twitter Order of December 14, 2010.[2] Finally, the issuance of a stay is in the public's interest because the public can have no interest in the enforcement of an unjustified nondisclosure provision and a stay will ensure that the user is afforded an opportunity to assert any constitutional or statutory rights he or she may have with regard to the Order.

[1] *See* Declaration of John K. Roche, Ex. 1 ("Roche Decl.") (filed Feb. 17, 2011).

[2] Roche Decl., Exs. 2-3.

I. ARGUMENT

A. The Court Should Grant a Stay of Production Pending Google's Appeal

1. Google Has Made a Strong Showing of Likely Success on the Merits

There is no dispute that the government's investigation of Wikileaks generally, and its interest in the [redacted] user name specifically, is a matter of public record. Moreover, as noted in Google's Reply in Support of its Objections, the government has offered no plausible justification for its assertion that disclosure of the Order will seriously jeopardize its investigation. Accordingly, Google respectfully submits it has a strong likelihood of success on the merits of this Court's *de novo*[3] review of Judge [redacted]'s ruling on Google's motion to modify the Order.

2. Google's Subscriber and Google Will Suffer Irreparable Injury Absent a Stay

The government claims that Google will not be injured absent a stay because "[t]he Order does not prevent Google from notifying the [redacted] subscriber forever." *See* Government Response, at 7. The point of Google's motion is to permit Google to notify its user before it produces anything to the government. Notification after the fact will be small solace to Google's user because by then the government will have spent the previous 3-5 months poring over his or her account records in the hope of finding "investigative leads" and "other subscriber information of which the government is unaware [which] might include transactional information helpful to obtain search warrant(s)." *See* Government Response, at 8-9. Moreover, despite the government's claims to the contrary, it is not at all clear that the user will in fact be able to challenge the introduction of these records in court at a later date. *U.S. v. Qing Li*, No. 07

[3] *U.S. v. Rosen*, 447 F. Supp. 2d 538, 545 (E.D. Va. 2006) (judicial orders based on sealed certifications from the government are reviewed *de novo*).

CR 2915 JM, 2008 WL 789899, at *3 (S.D. Cal. Mar. 20, 2008) (holding that the Stored Communications Act provides no suppression remedy) (collecting cases).

Furthermore, the government cannot seriously dispute the fact that the non-disclosure provision in the Order is a prior restraint on Google's First Amendment rights. *In re Sealing and Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 882 (S.D. Tex. 2008) ("a non-disclosure order imposes a prior restraint on speech."). The only question is whether the government can carry its "heavy burden of showing justification for the imposition of such a restraint." *Id.* (quoting *Capital Cities Media, Inc. v. Toole*, 463 U.S. 1303, 1305 (1983).

Google respectfully submits that because the government's interest in [redacted] electronic communications is already so well-publicized and there is absolutely no risk of destruction of evidence, the balance tips decidedly in favor of Google's First Amendment rights. Accordingly, Google and its user will suffer irreparable injury absent a stay.

3. A Stay Will Not Injure the Government or Harm the Public Interest

The government conceded it would not be injured by a stay when it moved to delay the hearing on Google's original motion until after Judge [redacted] had an opportunity to rule on the motions raised in regard to the Twitter Order. Judge [redacted] has had those motions under advisement for nearly three weeks now, and the government utterly fails to explain why it suddenly needs the documents immediately when it previously indicated it would be satisfied to wait until a ruling from Judge [redacted] in the Twitter matter. This unexplained contradiction is enough to establish that the government has no urgent need for these records and will not be injured by a stay. In addition, Google has preserved the responsive records so there is no danger that the data will be lost while this Court addresses the underlying Objections. It follows then that if the government admittedly has no urgent need for these records and the records are not at

risk of loss, there will be no harm to "the public interest in effective law enforcement and efficient administration of the criminal justice system" as the government claims. *See* Government Response, at 9.

II. CONCLUSION

For the reasons stated, Google requests an order to stay production of records and information in response to the Order while its concurrently filed Objections are pending.

DATED this 7th day of March, 2011.

Respectfully submitted,

By

John K. Roche (VSB# 68594)
Perkins Coie LLP
700 13th St., N.W., Suite 600
Washington, D.C. 20005-3960
Phone: 202-434-1627
Fax: 202-654-9106
JRoche@perkinscoie.com

Albert Gidari (*admitted pro hac vice*)
Perkins Coie LLP
1201 Third Avenue, Suite 4800
Seattle, Washington 98101
Phone: 206-359-8000
Fax: 206-359-9000
AGidari@perkinscoie.com

Attorneys for Google Inc.

CERTIFICATE OF SERVICE

I hereby certify that on this 7th day of March, 2011, the foregoing document was sent via hand delivery and email to the following persons:

[redacted]
Assistant United States Attorney
United States Attorney's Office
Eastern District of Virginia
Justin W. Williams United States Attorney's Building
2100 Jamieson Avenue
Alexandria, VA 22314-5794
703-299[redacted]
703-299[redacted] (facsimile)

Attorneys for the United States

By _____
John K. Roche (VSB# 68594)
Perkins Coie, LLP
700 13th St., N.W., Suite 600
Washington, D.C. 20005-3960
Phone: 202-434-1627
Fax: 202-654-9106
JRoche@perkinscoie.com

Attorneys for Google Inc.

ATTACHMENT L

THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

FILED
2011 MAR 22 P 3:33
CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

IN THE MATTER OF THE 2703(d) ORDER AND 2703(f) PRESERVATION REQUEST RELATING TO GMAIL ACCOUNT	Case No. 1:10GJ3793 - 11-DM-2 **UNDER SEAL** Hearing: March 24, 2011 (TSE)

NOTICE OF RELEVANT DECISION

The United States hereby provides the Court and opposing counsel with notice of a decision relevant to Google Inc.'s objections to Magistrate Judge [redacted] decision ("Google's Objections") that the court-ordered legal process for business records pursuant to the Stored Communications Act ("SCA") (18 U.S.C. §§ 2701-12) should remain under seal and not be disclosed for a limited period of time pending the ongoing criminal investigation.

In support of Google's Objections, Google explained that "three of the users identified in the Twitter Order, including Twitter's [redacted] user, filed a motion to vacate that order on Constitutional and statutory grounds." Google Obj. at 12; Google Reply. at 5. Google also argued that it is "reasonable to assume that the user may wish to assert similar objections to this Order." Google Obj. at 13. Therefore, the United States provides notice that on March 11, 2011, Magistrate Judge [redacted] issued the attached Memorandum Opinion and Order concerning the Twitter Order.

Respectfully Submitted,

[redacted]
United States Attorney

By: [redacted]
Assistant United States Attorney

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing pleading was delivered on this 22nd day of March 2011 to the Clerk's Office and that service will be made on the following individuals by electronic mail:

John K. Roche, Esquire
Perkins Coie LLP
700 13th St., N.W., Suite 600
Washington, D.C. 20005-3960
PHONE: 202.434.1627
FAX: 202.654.9106
E-MAIL: JRoche@perkinscoie.com

[redacted]
Assistant United States Attorney

Unsealed

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

In Re: §2703(d) Order; 10GJ3793	)	Miscellaneous No. 1:11dm00003

MEMORANDUM OPINION

This matter came before the Court the Motion of Real Parties in Interest Jacob Appelbaum, Birgitta Jonsdottir, and Rop Gonggrijp to Vacate December 14, 2010 Order ("Motion to Vacate", Dkt. 1) and Motion of Real Parties in Interest Jacob AppelBaum, Rop Gonggrijp, and Birgitta Jonsdottir for Unsealing of Sealed Court Records. ("Motion to Unseal", Dkt. 3). For the following reasons, petitioners' Motion to Vacate is DENIED, and petitioners' Motion to Unseal is DENIED in part, GRANTED in part, and taken under further consideration in part.

BACKGROUND

Petitioners are Twitter users associated with account names of interest to the government. Petitioner Jacob Appelbaum (Twitter name "ioerror") is a United States citizen and resident, described as a computer security researcher. (Pet. Motion to Unseal at 3). Rop Gonggrijp (Twitter name "rop_g") is a Dutch citizen and computer security specialist. *Id.* Birgitta

Jonsdottir (Twitter name "birgittaj") is an Icelandic citizen and resident. She currently serves as a member of the Parliament of Iceland. *Id.*

On December 14, 2010, upon the government's *ex parte* motion, the Court entered a sealed Order ("Twitter Order") pursuant to 18 U.S.C. § 2703(d) of the Stored Communications Act, which governs government access to customer records stored by a service provider. 18 U.S.C. §§ 2701-2711 (2000 & Supp. 2009). The Twitter Order, which was unsealed on January 5, 2010, required Twitter, Inc., a social network service provider, to turn over to the United States subscriber information concerning the following accounts and individuals: Wikileaks, rop_g, ioerror, birgittaj, Julian Assange, Bradely Manning, Rop Gonggrijp, and Birgitta Jonsdottir. In particular, the Twitter Order demands:

A. The following customer or subscriber account information for each account registered to or associated with Wikileaks; rop_g; ioerror; birgittaj; Julian Assange; Bradely Manning; Rop Gongrijp [*sic.*]; Birgitta Jonsdottir for the time period November 1, 2009 to present:
   1. subscriber names, user names, screen names, or other identities;
   2. mailing addresses, residential addresses, business addresses, e-mail addresses, and other contact information;
   3. connection records, or records of session times and durations;
   4. length of service (including start date) and types of service utilized;
   5. telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
   6. means and source of payment for such service (including any credit card or bank account number) and billing records.

B. All records and other information relating to the account(s) and time period in Part A, including:
   1. records of user activity for any connections made to or from the Account, including date, time, length, and method of connections, data transfer volume, user name, and source and destination Internet Protocol address(es);
   2. non-content information associated with the contents of any communication or file stored by or for the account(s), such as the source and destination email addresses and IP addresses.
   3. correspondence and notes of records related to the account(s).

On January 26, 2011, petitioners filed the instant motions asking the Court to vacate the Twitter Order, and to unseal all orders and supporting documents relating to Twitter and any other service provider. Moreover, petitioners request a public docket for each related order. On February 15, 2011, the Court held a public hearing and took petitioners' motions under consideration. For the following reasons, the Court declines to vacate the Twitter Order, and orders that only documents specified below shall be unsealed.

ANALYSIS

I. Motion to Vacate

Petitioners request that the Twitter Order be vacated. The parties have raised the following issues in their briefs: (1) whether petitioners have standing under the Stored Communications Act ("SCA") to bring a motion to vacate, (2) whether the Twitter Order was properly issued under 18 U.S.C. §2703, (3) whether the Twitter Order violates petitioners' First Amendment rights, (3)

whether the Twitter Order violates petitioners' Fourth Amendment rights, and (4) whether the Twitter Order should be vacated as to Ms. Jonsdottir for reasons of international comity.

(1) Petitioners' Standing Under 18 U.S.C. §2704(b)

Pursuant to §2704(b)(1)(A), a customer may challenge a §2703(d) order only upon an affidavit "stating that the applicant is a customer or subscriber to the service from which the *contents* of electronic communications maintained for him have been sought." (emphasis supplied). The Court holds that targets of court orders for non-content or records information may not bring a challenge under 18 U.S.C. §2704, and therefore, petitioners lack standing to bring a motion to vacate the Twitter Order.

The SCA provides greater protection to the "contents of electronic communications", sought pursuant to §2703(a) and §2703(b), than to their "records" (§2703(c)). The statutory definition of "contents" is "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. §2711(1); 18 U.S.C. §2510(8)(2002). Targets of content disclosures are authorized to bring a customer challenge under §2704. Conversely, §2703(c)(1) describes "records" as "a record or other information pertaining to a subscriber to or customer of such service (not the contents of communication)." According to §2703(c)(2), records include:

> (A) name;
> (B) address;
> (C) local and long distance telephone connection records, or records of session times and durations;

> (D) length of service (including start date) and types of service utilized;
> (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
> (F) means and source of payment for such service (including any credit card or bank account number), of a subscriber to or customer of such service when the governmental entity uses...*any means available under paragraph* (1) (emphasis supplied).

The Twitter Order does not demand the contents of any communication, and thus constitutes only a request for records under §2703(c). Even though the Twitter Order seeks information additional to the specific records listed in §2703(c)-- data transfer volume, source and destination Internet Protocol addresses, and [Twitter's] correspondence and notes of records related to the accounts -- these, too, are non-content "records" under §2703(c)(1). Therefore, as the targets of mere records disclosure, petitioners may not bring a customer challenge under §2704.

Petitioners, unable to overcome the language of §2704, assert in reply that they have standing based on general due process, but cite no authority on point. Moreover, §2704 seems to recognize that only targets of content disclosures would have a viable constitutional challenge to the compelled disclosure of private communications. Customers who voluntarily provide non-content records to an internet service provider would not enjoy the same level of protection.

(2) Proper Issuance of the Twitter Order

Notwithstanding petitioners' lack of standing to bring their motion to vacate, the Court finds that the substance of their motion is equally unavailing.

The Twitter Order came before the Court upon the government's motion and supporting application for an order pursuant to 18 U.S.C. §2703(d). Section 2703(d) provides in pertinent part:

> "(d) Requirements for court order.--A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are *relevant and material* to an ongoing criminal investigation." (emphasis supplied).

On December 14, 2010, the Court found that the application satisfied §2703(d) and entered the Twitter Order. Petitioners now ask the Court to reconsider the sufficiency of the underlying application pursuant to §2704(b)(1)(B), which authorizes customers to move to vacate an order upon a showing "that there has not been substantial compliance" with §2703(d). Because the application remains sealed, petitioners face the difficulty of challenging a document they have not seen. Nevertheless, petitioners speculate that regardless of the application's factual support, it could not have justified the scope of the Twitter Order. That is, petitioners contend that because their publically posted "tweets" pertained mostly to non-Wikileaks topics, the Twitter Order necessarily demands data that has no connection to Wikileaks and cannot be "relevant or material" to any ongoing investigation as §2703(d) requires. Notwithstanding

petitioners' questions, the Court remains convinced that the application stated "specific and articulable" facts sufficient to issue the Twitter Order under §2703(d). The disclosures sought are "relevant and material" to a legitimate law enforcement inquiry. Also, the scope of the Twitter Order is appropriate even if it compels disclosure of some unhelpful information. Indeed, §2703(d) is routinely used to compel disclosure of records, only some of which are later determined to be essential to the government's case. Thus, the Twitter Order was properly issued pursuant to §2703(d).

As an alternative, petitioners propose that, even if the government has stated facts sufficient to meet the §2703(d) "relevant and material" standard, the Court should use its discretion to require the government to meet the probable cause standard required for a search warrant. *See In re Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304, 315-17 (3d Cir. 2010). The Court declines to deviate from the standard expressly provided in §2703(d). At an early stage, the requirement of a higher probable cause standard for non-content information voluntarily released to a third party would needlessly hamper an investigation. *See In re Subpoena Duces Tecum*, 228 F.3d 341, 348-39 (4th Cir. 2000). Therefore, the Court finds that the Twitter Order was properly issued.

(3) First Amendment Claim

Petitioners claim the Twitter Order allows the government to create a "map of association" that will have a chilling effect on their First Amendment rights.[1]

The First Amendment guarantees freedom of speech and assembly.[2] Recognizing the "close nexus between freedoms of speech and assembly", the Supreme Court has established an implicit First Amendment right to freely associate. *N.A.A.C.P. v. Alabama ex rel. Patterson*, 357 U.S. 449,460 (1958). The freedom of association may be hampered by compelled disclosure of a political or religious organization's membership. *Id.* at 462 (preventing compelled disclosure of NAACP membership list). However, the freedom of association does not shield members from cooperating with legitimate government investigations. *United States v. Mayer*, 503 F.3d 740, 748 (9th Cir. 2007). Other First Amendment interests also yield to the investigatory process. *Brazenburg v. Hayes*, 408 U.S. 665, 682, 691 (1972)(freedom of the

---

[1]Though they assert First and Fourth Amendment claims, petitioners cite no authority as to the applicability of the United States Constitution to non-citizens residing and acting outside of the U.S. *See United States v. Verdugo-Urquidez*, 494 U.S. 259, 265 (1990)(Fourth Amendment inapplicable where American authorities searched the home of a Mexican citizen and resident, who had no voluntary attachment to the United States; *Wang v. Reno*, 81 F.3d 808,817-18 (9th Cir. 1996)(alien entitled to 5th Amendment due process rights only after government created "special relationship with alien" by paroling him from China to U.S. to testify at drug trial). The Court has serious doubts as to whether Ms. Jonsdottir and Mr. Gonggrijp enjoy rights under the U.S. Constitution.

[2]"Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." U.S. CONST. amend. I.

press); *University of Pennsylvania v. E.E.O.C.*, 493 U.S. 182, 197-98 (1990)(academic freedom). In the context of a criminal investigation, a district court must "balance the possible constitutional infringement and the government's need for documents...on a case-by-case basis and without putting any special burden on the government", and must also prevent abuse. *In re Grand Jury 87-3 Subpoena Duces Tecum*, 955 F.2d 229,234 (4th Cir. 1992).[3] Accordingly, a subpoena should be quashed where the underlying investigation was instituted or conducted in bad faith, maliciously, or with intent to harass. *Id.*[4]

The Court finds no cognizable First Amendment violation here. Petitioners, who have already made their Twitter posts and associations publicly available, fail to explain how the Twitter Order has a chilling effect. The Twitter Order does not seek to control or direct the content of petitioners' speech or association. Rather, it is a routine compelled disclosure of non-content information which petitioners voluntarily provided to Twitter pursuant to Twitter's Privacy Policy. Additionally, the

---

[3]Other circuits have adopted a "substantial relationship" test, whereby the government must show its subpoena serves a compelling interest that outweighs any alleged chilling effect. But even courts that have adopted the test regularly refuse to quash subpoenas on First Amendment grounds. *See In re Grand Jury Proceedings*, 776 F.2d 1099,1103 (2d Cir. 1985)(requiring cooperation with pre-indictment proceedings); *In re Grand Jury Subpoenas Duces Tecum*, 78 F.3d 1307, 1312-13(8th Cir. 1996)(same); *In re Grand Jury Proceedings*, 842 F.2d 1229,1236-37 (11th Cir. 1988)(same).

[4]Most cases dealing with First Amendment challenges in the pre-indictment phase involve subpoenas, not §2703(d) court orders. However, §2703(d) orders resemble subpoenas because they also compel disclosure of documents.

Court's §2703(d) analysis assured that the Twitter Order is reasonable in scope, and the government has a legitimate interest in the disclosures sought. *See In re Grand Jury 87-3 Subpoena Duces Tecum*, 955 F.2d at 234. Furthermore, there is no indication of bad faith by the government. *Id.* Thus, petitioners' First Amendment challenge to the Twitter Order fails.

(4) Fourth Amendment Claim

Petitioners argue that the Twitter Order should be vacated because it amounts to a warrantless search in violation of the Fourth Amendment. In particular, petitioners challenge the instruction that Twitter, Inc. produce the internet protocol addresses ("IP addresses") for petitioners' Twitter accounts for specified dates and times. Petitioners assert a Fourth Amendment privacy interest in their IP address information, which they insist are "intensely revealing" as to location, including the interior of a home and movements within.

The Fourth Amendment provides that "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..." U.S. CONST. amend. IV. Not all investigatory techniques by the government implicate the Fourth Amendment. A government action constitutes a "search" only if it infringes on an expectation of privacy that society considers reasonable. *United States v. Jacobsen*, 466 U.S. 109,113 (1984). Thus, the government must obtain a warrant before inspecting places where the public

traditionally expects privacy, like the inside of a home or the contents of a letter. *United States v. Karo*, 468 U.S. 705, 714 (1984) (warrant required to use electronic location-monitoring device in a private home); *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (warrant required to use publically unavailable, sense-enhancing technology to gather information about the interior of a home); *Jacobsen*, 466 U.S. at 114 (warrant required to inspect the contents of sealed letters and packages); *See also United States v. Warshak*, 2010 WL 5071766 at 13-14 (6th Cir. 2010) (extending Fourth Amendment protection to the contents of certain email communications).

On the other hand, the Fourth Amendment privacy expectation does not extend to information voluntarily conveyed to third parties. For example, a warrantless search of bank customers' deposit information does not violate the Fourth Amendment, because there can be no reasonable expectation of privacy in information voluntarily conveyed to bank employees. *United States v. Miller*, 425 U.S. 435, 442 (1976). Similarly, the Fourth Amendment permits the government to warrantlessly install a pen register to record numbers dialed from a telephone because a person voluntarily conveys the numbers without a legitimate expectation of privacy. *Smith v. Maryland*, 442 U.S. 735 (1979).

With these principles in mind, the Fourth Circuit has held that no legitimate expectation of privacy exists in subscriber information voluntarily conveyed to phone and internet companies. *United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010) (citing *Smith v. Maryland*, 442 U.S. at 744). In *Bynum*, the defendant,

who was convicted of child pornography charges, challenged the constitutionality of administrative subpoenas the government used to collect information from his internet and phone companies, including his name, email address, phone number, and physical address. *Id.* Holding that the subpoenas did not violate the Fourth Amendment, the *Bynum* Court reasoned that the defendant had no expectation of privacy in information he voluntarily conveyed, and that in doing so, he assumed the risk that the companies would turn it over to authorities. *Id.* Moreover, "every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment." *Id.* at 164. Accordingly, several circuits have declined to recognize a Fourth Amendment privacy interest in IP addresses.[5] *United States v. Christie*, 624 F.3d 558,574 (3d Cir. 2010)("no reasonable expectation of privacy exists in an IP address, because that information is also conveyed to and, indeed, from third parties, including ISPs"); *United States v. Forrester*, 512 F.3d 500,510 (9th Cir. 2008); *United States v. Perrine*, 518 F.3d 1196, 1204-05 (10th Cir. 2008); *see also Bynum*

---

[5] Petitioners highlight the Supreme Court's admonition that courts should avoid unnecessary rulings on how the Fourth Amendment applies to new technologies. *City of Ontario v. Quon*, 130 S. Ct. 2619, 2629, 177 L. Ed. 2d 216 (2010). There, in a case involving employer-provided electronic communication devices, the Court said "the judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear". Here several courts have encountered IP address issues. This is not "emerging technology" worthy of constitutional avoidance.

604 F.3d at 164 n.2 (stating that defendant's IP address amounts to numbers that he "never possessed").

Here, petitioners have no Fourth Amendment privacy interest in their IP addresses. The Court rejects petitioners' characterization that IP addresses and location information, paired with inferences, are "intensely revealing" about the interior of their homes. The Court is aware of no authority finding that an IP address shows location with precision, let alone provides insight into a home's interior or a user's movements. Thus the *Kyllo* and *Karo* doctrines are inapposite. Rather, like a phone number, an IP address is a unique identifier, assigned through a service provider. *Christie*, 624 F.3d at 563; *Smith v. Maryland*, 442 U.S. at 744. Each IP address corresponds to an internet user's individual computer. *Christie*, 624 F.3d at 563. When a user visits a website, the site administrator can view the IP address. *Id.* Similarly, petitioners in this case voluntarily conveyed their IP addresses to the Twitter website, thus exposing the information to a third party administrator, and thereby relinquishing any reasonable expectation of privacy.

In an attempt to distinguish the reasoning of *Smith v. Maryland* and *Bynum*, petitioners contend that Twitter users do not directly, visibly, or knowingly convey their IP addresses to the website, and thus maintain a legitimate privacy interest. This is inaccurate. Before creating a Twitter account, readers are notified that IP addresses are among the kinds of "Log Data" that Twitter collects, transfers, and manipulates. *See Warshak*, 2010

WL 5071766 at *13 (recognizing that internet service provider's notice of intent to monitor subscribers' emails diminishes expectation of privacy). Thus, because petitioners voluntarily conveyed their IP addresses to Twitter as a condition of use, they have no legitimate Fourth Amendment privacy interest. *Smith*, 422 U.S. at 744; *Bynum*, 604 F.3d at 164.[6]

(5) International Comity

Petitioners argue the Twitter Order should be vacated as to Ms. Jonsdottir, a member of the Icelandic Parliament.[7] Petitioners warn of a threat to international comity, which is defined as "the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens or of other persons who are under the protection of its laws." *In re French v. Liebmann*, 440 F.3d 145,152 (4th Cir. 2006)(*citing Hilton v. Guyot*, 159 U.S. 113, 164 (1895).

---

[6]At the hearing, petitioners suggested that they did not read or understand Twitter's Privacy Policy, such that any conveyance of IP addresses to Twitter was involuntary. This is unpersuasive. Internet users are bound by the terms of click-though agreements made online. *A.V. ex rel. Vanderhye v. iParadigms, LLC*, 544 F.Supp.2d 473,480 (E.D. Va. 2008)(finding a valid "clickwrap" contract where users clicked "I Agree" to acknowledge their acceptance of the terms)(*aff'd A.V. ex rel v. iParadigms, LLC*, 562 F.3d 630,645 n.8 (4th Cir. 2009). By clicking on "create my account", petitioners consented to Twitter's terms of use in a binding "clickwrap" agreement to turn over to Twitter their IP addresses and more.

[7]The Court thanks the Inter-Parliamentary Union for its *Amicus* Brief on this issue.

The threshold question in international comity analysis is whether there is a conflict between foreign and domestic law. *Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court.*, 482 U.S. 522, 555 (1987). A corollary of international comity is the established presumption against extraterritorial application of American statutes. *In re French*, 440 F.3d at 149, 151.

Here, petitioners have not asserted any conflict between American and Icelandic Law implicating international comity concerns. Instead, petitioners assert that the disclosures sought could not be obtained under Icelandic law, which affords strong immunity to members of parliament. According to the Inter-Parliamentary Union, Icelandic parliamentary immunity "ensures that members of parliament cannot be held to account for the opinions they express and the votes they cast..." (Sears Decl. Ex. 6). Here, the Twitter Order does not violate this provision. It does not ask Ms. Jonsdottir to account for her opinions. It does not seek information on parliamentary affairs in Iceland, or any of Ms. Jonsdottir's parliamentary acts. Her status as a member of parliament is merely incidental to this investigation. Also, neither petitioners nor the Inter-Parliamentary Union have cited authority to support their assumption that Icelandic immunity extends to public "tweets". In the United States, such public statements are not regarded as part of the legislative function or process, and thus would not invoke the legislative immunity of the Constitution's Speech and Debate Clause. *Hutchinson v. Proxmire*, 443 U.S. 111, 132 (1979)(no legislative immunity for statements "scattered far and

wide by mail, press, and the electronic media"); *United States v. Gravel*, 408 U.S. 606, 616 (1972). Nor would a member of Congress be permitted to invoke her position to avoid being a witness in a criminal case. *Gravel*, 408 U.S. at 622. Thus, the Court rejects the assertion that the Twitter Order is a clash of American and Icelandic law that threatens international comity.

Moreover, in accordance with international comity, the Twitter Order is not an extraterritorial application of American law. Rather, it is a routine request for information pursuant to a valid act of the United States Congress, the Stored Communications Act. It compels disclosures from Twitter, an American corporation, and requires nothing of Ms. Jonsdottir. When Ms. Jonsdottir consented to Twitter's Privacy Policy she assumed the risk that the United State's government could request such information. For these reasons, the Court declines to vacate the Twitter Order as to Ms. Jonsdottir.

II. Motion to Unseal

The documents in this matter, 1:11-dm-00003, were initially sealed by the Clerk's office. Petitioners now ask that all documents within this file be unsealed. According to the parties' agreement, sealing is no longer necessary for the 1:11-dm-00003 docket, with the exception of Government's Response in Opposition to the Real Parties' in Interest Motion for Unsealing of Sealed Court Records (Dkt. 22) and Twitter's Motion for Clarification (Dkt. 24), to which the government still objects.

Petitioners further request the unsealing of the application in support of the Twitter Order and all other documents in case

number 10-gj-3793. Additionally, to the extent any other companies received similar orders, petitioners request the unsealing of those orders and their applications. Petitioners also request a public docket of such material.

Petitioners have no right of access to the sealed documents supporting the Twitter Order in case number 10-gj-3793. At the pre-indictment phase, "law enforcement agencies must be able to investigate crime without the details of the investigation being released to the public in a manner that compromises the investigation." *Va. Dept. of State Police v. Washington Post*, 386 F.3d 567, 574 (4th Cir. 2004). Secrecy protects the safety of law enforcement officers and prevents destruction of evidence. *Media General Operations v. Buchanan*, 417 F.3d 424,429 (4th Cir. 2005). It also protects witnesses from intimidation or retaliation. *In re Grand Jury Investigation of Cuisinarts, Inc.*, 665 F.2d 24, 27-28 (2d Cir. 1981). Additionally, secrecy prevents unnecessary exposure of those who may be the subject of an investigation, but are later exonerated. *Douglas Oil Co. V. Petrol Stops N.W.*, 441 U.S. 211, 219 (1979). For these reasons, sensitive investigatory material is appropriately sealed. *Va. Dept. of State Police*, 386 F.3d at 589.

In spite of these considerations, petitioners claim this material should be accessible pursuant to the common law presumption that public documents, including judicial records, are open and available for citizens to inspect. *Media General Operations v. Buchanan*, 417 F.3d 424, 429 (4th Cir. 2005)(citing *Nixon v. Warner Communications, Inc.*, 435 U.S. 589, 597-98

right of access only when (1) the place or process to which access is sought has been historically open to the public, and (2) public access plays a significant positive role in the particular process. *Baltimore Sun v. Goetz*, 886 F.2d 60, 63-64 (4th Cir. 1989). As set forth above, there is no history of openness for documents related to an ongoing criminal investigation. Additionally, there are legitimate concerns that publication of the documents at this juncture will hamper the investigatory process. Thus, there is no First Amendment justification for unsealing the 10-gj-3793 documents.

Concerning petitioners' request for public docketing of 10-gj-3793, this requires further review and will be taken under consideration.

Regarding case number 1:11-dm-00003, the Court has reviewed the redactions requested by the government as to docket numbers 22 and 24. As to the Government's Response in Opposition to the Real Parties' in Interest Motion for Unsealing of Sealed Court Records (Dkt. 22), the Court finds that the proposed redactions do not reveal any sensitive investigatory facts which are not already revealed by the Twitter Order. Therefore, it shall be unsealed. The government's remaining proposed redaction is the email address of a government attorney appearing on Twitter, Inc.'s Motion for Clarification. (Dkt. 24). The Court finds that this redaction is appropriate, and the redacted version of Twitter Inc.'s motion shall be released.

CONCLUSION

ATTACHMENT M

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

IN RE 2703(d) ORDER AND 2703(f) PRESERVATION REQUEST RELATING TO GMAIL ACCOUNT [redacted]	Misc. No. 10GJ3793 11-DM-2 FILED UNDER SEAL

GOOGLE INC.'S RESPONSE TO NOTICE OF RELEVANT DECISION[1]

Google Inc. ("Google") hereby responds to the government's Notice of Relevant Decision regarding Judge [redacted] Order and Memorandum Opinion denying the motion to vacate the Twitter Order.[2]

At the outset, Google notes that the Order and Memorandum Opinion do not affect whether the government met the § 2705(b) nondisclosure standard here when it unsealed an order the day before seeking the same information on the same account name from another provider.

Furthermore, at page 9, Judge [redacted] found "no cognizable First Amendment violation" because the Twitter users "have already made their Twitter posts and associations publicly available . . . ." Google respectfully submits this analysis would not apply to any First Amendment challenge brought by Google's [redacted] user because emails and contact lists in a Gmail account are not in any sense publicly available.

[1] In the absence of a formal rule governing supplemental authority, Google adheres to the 350-word count limitation in Fed. R. App. 28(j).

[2] *See* Declaration of John K. Roche, Ex. 2 ("Roche Decl.") (filed Feb. 17, 2011).

Finally, Google also respectfully submits that Judge [redacted]s conclusion that the Twitter users lack standing under 18 U.S.C. § 2704 (*see* Memorandum Opinion, at 4-5) would not foreclose a First Amendment challenge by Google's [redacted] user to the government's attempt to obtain his or her non-content records. *In re First Nat. Bank, Englewood, Colo.*, 701 F.2d 115, 118-19 (10th Cir. 1983) (organization and members had standing to challenge on First Amendment association grounds a grand jury subpoena issued to their bank); *Paton v. La Prade*, 524 F.2d 862, 873 (3d Cir. 1975) (individual had standing to raise First Amendment challenge to Postal Regulation authorizing "mail covers," *i.e.*, process by which Post Office copies address information on a suspect's mail and forwards to law enforcement); *cf. Amnesty International USA v. Clapper*, 09-4112-cv (2d Cir. Mar. 21, 2011) (slip op.) (individuals and organizations have standing to challenge § 702 of FISA on First and Fourth Amendment grounds).

At bottom, the user should have a chance to fully raise these arguments.

DATED this 23rd day of March, 2011.

Respectfully submitted,

By _____

John K. Roche (VSB# 68594)
Perkins Coie LLP
700 13th St., N.W., Suite 600
Washington, D.C. 20005-3960
Phone: 202-434-1627
Fax: 202-654-9106
JRoche@perkinscoie.com

Albert Gidari (*admitted pro hac vice*)
Perkins Coie LLP
1201 Third Avenue, Suite 4800
Seattle, Washington 98101
Phone: 206-359-8000
Fax: 206-359-9000
AGidari@perkinscoie.com

Attorneys for Google Inc.

CERTIFICATE OF SERVICE

I hereby certify that on this 23rd day of March, 2011, the foregoing document was sent via hand delivery and email to the following persons:

[redacted]
Assistant United States Attorney
United States Attorney's Office
Eastern District of Virginia
Justin W. Williams United States Attorney's Building
2100 Jamieson Avenue
Alexandria, VA 22314-5794
[redacted]

Attorneys for the United States

By _____
John K. Roche (VSB# 68594)
Perkins Coie, LLP
700 13th St., N.W., Suite 600
Washington, D.C. 20005-3960
Phone: 202-434-1627
Fax: 202-654-9106
JRoche@perkinscoie.com

Attorneys for Google Inc.

ATTACHMENT N

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

IN THE MATTER OF THE 2703(d) ORDER AND 2703(f) PRESERVATION REQUEST RELATING TO GMAIL ACCOUNT	)	**Misc. No. 1:10GJ3793**
	)	**11-DM-2**
	)	**UNDER SEAL**

MEMORANDUM OPINION

At issue in this sealed matter is whether the magistrate judge erred in issuing an order in connection with a grand jury investigation and pursuant to 18 U.S.C. § 2703(d) directing Google, Inc., an electronic communications service provider and remote computing service, to disclose certain noncontent business subscriber and transaction records concerning a particular subscriber of its service without disclosing the existence of the order to anyone, including the subscriber, for at least ninety days. For the reasons that follow, Google's objections to the magistrate judge's ruling are overruled in all respects.

I.

This matter arises out of the government's ongoing grand jury investigation of the alleged unlawful disclosure of state secrets through the website known as WikiLeaks (the "WikiLeaks investigation"). On January 4, 2011, the government applied for and was granted an order ("Google Order") from a United States magistrate judge pursuant to 18 U.S.C. § 2703(d) directing Google to provide the government the noncontent business subscriber and transaction records for the account associated with the email address "[redacted] account"), covering the time period from November 1, 2009 to present. *In re Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(d)*, No. 1:10GJ3793 (E.D. Va. Jan. 4, 2011) (Order). More specifically, the information ordered disclosed by the Google

Order includes, *inter alia*, contact information associated with the [redacted] account, records of user activity, and source and destination email addresses for any emails stored on the account—but not the actual content of any emails. The government also requested a provision in the Google Order pursuant to § 2705(b) barring Google from disclosing the existence of the order to anyone, a request the magistrate judge granted after finding that disclosure would "seriously jeopardiz[e] [the] investigation." *See* § 2705(b)(5).

The Google Order is not the only § 2703(d) order arising out of the government's WikiLeaks investigation. On December 14, 2010, before the issuance of the Google Order, a separate magistrate judge issued an order requiring Twitter, Inc. to disclose noncontent records for several Twitter accounts, including the account [redacted]" ("Twitter Order"). Like the Google Order, the Twitter Order originally barred disclosure of the order's existence, but at Twitter's request, the government subsequently consented to unsealing the order. After the Twitter Order was unsealed, Google then requested that the government consent to unsealing the Google Order as well. The government, however, did not consent to unsealing the Google Order entirely, agreeing instead to limit nondisclosure of the Google Order to ninety days, with an option for the government to extend the nondisclosure period an additional sixty days. Accordingly, on February 9, 2011, the magistrate judge modified the Google Order to include the ninety-day nondisclosure period with an optional sixty-day extension and rejected Google's argument that the order should be unsealed entirely. *In re 2703(d) Order and 2703(f) Preservation Request Relating to Gmail Account* [redacted] No. 1:10GJ3793 (E.D. Va. Feb. 9, 2011) (Order). Google objects to the magistrate judge's ruling, contending that the Google order should be unsealed and that Google should be permitted to notify the subscriber—in this

instance, [redacted]—of the order immediately. The government argues that the magistrate judge's ruling was appropriate in all respects and should not be modified.

II.

As always when reviewing a magistrate judge's order, it is appropriate to begin by identifying the proper the standard of review. Although the parties agree that the magistrate judge's ruling must be reviewed under Rule 59, Fed. R. Crim. P., they disagree about which subsection applies. The government contends that the ruling can only be modified if the ruling is "clearly erroneous or contrary to law standard," based on Rule 59(a). Google, on the other hand, contends that the ruling must be reviewed *de novo*, based on Rule 59(b).

Although the issue is one of first impression, a careful examination of Rule 59's text resolves the conflict in favor of the government. Rule 59(a) provides that objections to the determination of a magistrate judge on "any matter that does not dispose of a charge or defense" must be reviewed by the district court under a clearly erroneous or contrary to law standard. By contrast, Rule 59(b) provides that objections to dispositive matters—including "a defendant's motion to dismiss or quash an indictment or information, a motion to suppress evidence, or any matter that may dispose of a charge or defense"—must be reviewed by a district court *de novo*. *Id.* The government correctly recognizes that the magistrate judge's issuance of a § 2703(d) order is not a dispositive matter, and thus, under Rule 59(a), the order may be modified by the district court only if the order is clearly erroneous or contrary to law. As the government points out, the § 2703(d) order does not dispose of a charge or defense; rather, it merely orders the disclosure of material by a third party in the course of an ongoing investigation. As such, the order falls squarely within the scope of Rule 59(a). It is equally clear that the order does not fall within the scope of Rule 59(b) based on the text of that subsection, as the Google Order is not

analogous to an order on any of the matters enumerated in Rule 59(b), namely a motion to dismiss, a motion to suppress evidence, or a motion to quash an indictment.[1]

Google offers two additional arguments in support of its assertion that the magistrate judge's ruling concerned a dispositive matter under Rule 59(a). First, Google notes that in *United States v. Myers*, 593 F.3d 338 (4th Cir. 2010), the Fourth Circuit held that it had jurisdiction to hear the interlocutory appeal of a discovery order directed at a disinterested third party because such an order is treated as an immediately appealable final order as to that third party. *Id.* at 345. Yet, the mere fact that an order is considered final as to a third party and thus subject to interlocutory appeal is irrelevant to whether the matter is "dispositive" within the meaning of Rule 59, Fed. R. Crim. P. The question here is simply whether the magistrate judge's ruling disposes of a charge or defense, and it clearly does not. Whether Google may seek an interlocutory appeal in this matter is a separate issue entirely that is neither raised nor necessary to address here.

Next, Google cites *United States v. Rosen*, 447 F. Supp. 2d 538 (E.D. Va. 2006), which, *inter alia*, reviewed a probable cause determination of a Foreign Intelligence Surveillance Court ("FISC") *de novo*. As an initial matter, *Rosen* did not conduct any analysis of the standard of review, noting instead that even under the least deferential standard of review—*i.e., de novo* review—the FISC judge's probable cause determination in that case was correct. *Id.* at 545. More importantly, the statutory scheme governing Foreign Intelligence Surveillance Act

---

[1] The government also notes that a court's decision to seal is generally reviewed only for abuse of discretion. *See Baltimore Sun Co. v. Goetz*, 886 F.2d 60, 65 (4th Cir. 1989) ("The judicial officer's decision to seal, or to grant access, is subject to review under an abuse of discretion standard."). Yet, the magistrate judge's ruling here is not simply an order sealing a pleading, but rather a broader nondisclosure order pursuant to 18 U.S.C. § 2703(d). Accordingly, as the parties agree, it is appropriate to review the magistrate judge's ruling under Rule 59 rather than principles governing sealing orders under *Baltimore Sun*.

warrants is entirely distinct from the statutory scheme in issue here. *Compare* 50 U.S.C. §§ 1805, 1806, 1825 *with* 18 U.S.C. §§ 2703, 2705. Thus, the *Rosen* decision does not inform the analysis here. Instead, the analysis is appropriately guided by the plain language of Rule 59, Fed. R. Crim. P. Accordingly, the Google Order will only be modified if it is clearly erroneous or contrary to law.[2]

III.

Analysis of Google's objections to the magistrate judge's ruling begins with a brief review of the relevant provisions of the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701 *et seq*. The SCA permits the government to seek access to customer records stored by the providers of electronic communication or remote computing services. *See* 18 U.S.C. § 2703. Under § 2703(c)(1), a governmental entity may

> require a provider of electronic communication service or remote computing service . . . to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) . . . .

The SCA further provides that the government may apply for an order compelling service providers to disclose this information by demonstrating to a court "specific and articulable facts showing that there are reasonable grounds to believe . . . the records or other information sought, are relevant and material to an ongoing criminal investigation." § 2703(d). If the government seeks only noncontent information, the government is not required to notify the subscriber of the account in issue of the order's existence. *See* § 2703(c)(3). Importantly, under § 2705(b), the government may also request—as it did here—that the court bar the service provider from disclosing the existence of the § 2703(d) order. Such a request may be granted if the court

---

[2] Nevertheless, while it is not necessary to review the magistrate judge's ruling *de novo*, such a review has been conducted here and reveals no basis on which to modify the magistrate judge's ruling. Thus, as explained *infra*, even were Google correct about the standard of review, its objections would be overruled.

"determines that there is reason to believe that notification of the existence" of the order "will result" in, *inter alia*, "seriously jeopardizing an investigation." § 2705(b).[3] The statute also allows a service provider to move to quash or modify the 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." § 2703(d). Significantly, the statute allows no other grounds on which the service provider may challenge the order.

There is no dispute that the appropriate statutory procedures were followed by the government in obtaining the Google Order and the accompanying nondisclosure provision. The magistrate judge found that a disclosure bar was appropriate only after the government demonstrated that disclosure would seriously jeopardize its investigation. Nevertheless, Google objects to the magistrate judge's ruling barring disclosure of the Google Order on three grounds. First, Google argues that because the Twitter Order has already been unsealed, the investigation cannot be further jeopardized by disclosure of the Google Order. Second, Google contends that the Google Order may raise significant constitutional and statutory issues that the [redacted]account holder should have an opportunity to assert before the order is executed. Finally, Google argues that the nondisclosure provision constitutes an unlawful prior restraint on Google's First Amendment right to free speech. In response, the government contends that the statute does not permit a service provider to challenge a § 2703(d) order on the grounds asserted by Google, and in any event, that Google's arguments are meritless. A careful examination of the statute and the

---

[3] The statute recognizes that a nondisclosure order may be justified if disclosure would result in any of the following: (i) endangering the life or physical safety of an individual; (ii) flight from prosecution; (iii) destruction of or tampering with evidence; (iv) intimidation of potential witnesses; or (v) otherwise seriously jeopardizing an investigation or unduly delaying a trial. *See* § 2705(b). The government relies on the fifth ground—seriously jeopardizing an investigation—to justify the nondisclosure provision in issue here.

record confirms that the government is correct, both as to Google's limited standing to challenge the nondisclosure provision and as to the merits of Google's arguments.

It is appropriate to begin with the government's argument that Google's objections to the nondisclosure provision are not permitted by the statute. Section 2703(d) states that a service provider may move to quash or modify the given order on two grounds, namely that the requested records are "unusually voluminous" or that compliance with the request would cause an "undue burden." The government argues that these enumerated grounds for a motion to quash or modify are the only grounds available to service providers for challenging a § 2703(d) order. The text of the statute supports the government's conclusion. Section 2703(d) plainly states that the motion to quash or modify may be brought "if" one of the two enumerated grounds are applicable. The enumeration of two, and only two, grounds for challenging the order implies—under the "time-honored maxim" *expressio unius est exclusio alterius*[4]—that no other grounds may serve as the basis for a motion to quash or modify the order. Had Congress wished to authorize a service provider to assert other grounds to challenge the order, it easily could have done so either by enumerating those additional grounds or by noting that the list was not exhaustive.[5] Congress did neither in the SCA, and its failure to do so must be regarded as a clear statement of its intent not to recognize further bases for service providers' challenges to a § 2703(d) order.

---

[4] *See Ayes v. U.S. Dep't of Veterans Affairs*, 473 F.3d 104, 111 (4th Cir. 2006) (applying the "time-honored maxim *expressio unius est exclusio alterius* ('the expression of one thing implies the exclusion of another')" to find that Congress's failure to include veteran guaranty entitlements from among the list of grants enumerated in the antidiscrimination provision of the Bankruptcy Code, 11 U.S.C. § 252(a), meant that such entitlements were beyond the scope of that statute).

[5] For example, statutes often insert the word "including" before a list of examples when the list is nonexclusive. *See, e.g., West v. Gibson*, 527 U.S. 212, 218 (1999) (in analyzing the Title VII remedies statute, noting that Congress's use of the word "including" makes clear the list is not exhaustive).

Without conceding this conclusion, Google argues that even if the "voluminous records" and "undue burden" grounds are the only acceptable bases for challenging the magistrate judge's ruling, Google's arguments nonetheless may be heard because they fit within the scope of the "undue burden" provision. To reach this result, Google repackages its arguments as supporting the broad proposition that Google would suffer an undue burden if it were forced to comply with a nondisclosure order that is not adequately supported by fact or law. Google Reply Br. at 3.

The SCA's clear text fully refutes this argument. Significant in this regard is the placement of the word "otherwise" in the statutory text. Thus, the statute states that a service provider may move to quash or modify the 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." § 2703(d) (emphasis added). The use of "otherwise" following the reference to "unusually voluminous" indicates—based on the maxim of *ejusdem generis*—that the only types of burdens contemplated by the statute are those similar in nature to the burdens imposed by a request for unusually voluminous records.[6] Such burdens would ostensibly include technical and logistical burdens involved in complying with the § 2703(d) order, but not Google's purported "burden" of complying with an order that, in its view, lacks a firm basis in law or fact. Were the statute read as Google suggests, the phrase "undue burden" would be broad enough to encompass any objection a service provider might imagine, thus rendering the conditional language of § 2703(d) a nullity. Accordingly, because none of Google's grounds for challenging the order are technical or logistical in nature, Google's objections to the magistrate judge's ruling must be overruled.

---

[6] *See id.* at 109 n.3 ("When general words follow specific words in a statutory enumeration, we apply the interpretive principle of *ejusdem generis* ('of the same kind') and construe the general words to embrace only objects similar in nature to those objects enumerated by the preceding specific words.") (quotations and ellipsis omitted).

Nevertheless, even if one considers the merits of Google's objections, it is clear that the objections must be still overruled. Google's first objection—and certainly its most vigorously advanced objection—is that, as a factual matter, the government has failed to meet its burden of showing that disclosure of the Google Order would seriously jeopardize the government's ongoing investigation. Google essentially argues that no further injury to the government's investigation can occur beyond that which has already occurred owing to publication of the Twitter Order. Consideration of this argument must begin with an understanding of the harm purportedly caused by the unsealing of the Twitter Order itself, harm the government asserts would be compounded if the Google Order were also unsealed.

The record reflects that after the Twitter Order was unsealed, the holder of the [redacted] Twitter account posted an online message indicating that other Twitter users should not send him or her direct messages over the Twitter service because the account was being monitored by the government.[7] Given this, the government contends that because unsealing the Twitter Order apparently caused the subscriber to alter his or her behavior, it follows that unsealing the Google Order could similarly lead to a change in the email usage of whatever entity or person operates the [redacted] email account with Google.[8] This concern is well founded. Even if the [redacted] account holder already suspects that the government seeks information from his or her email

---

[7] Direct messages must be distinguished from general messages—or "tweets"—on the Twitter website. A direct message is a message sent privately from one Twitter user to another. Tweets are messages broadcasted publicly by one Twitter user to any and all users who may wish to view—*i.e.*, "follow"—the user's tweets.

[8] Although the government and Google suggested in oral argument that it may be likely that the same individual maintains both the [redacted] Twitter account and the [redacted]mail.com email account, this fact is not confirmed in this record, and in any event, is immaterial to the analysis here.

account, it is reasonable to expect that *confirmation* of this fact would prompt yet additional steps by this subscriber to avoid government monitoring of his or her accounts or other activities.

In response, Google notes that the Google Order only seeks historical, not prospective, data, and that Google has already preserved this data, such that any potential change in the subscriber's future email behavior caused by unsealing the Google Order is immaterial. What this argument critically fails to recognize is that the government's investigation is ongoing, and any change in the suspect's behavior, whether with respect to internet usage or otherwise, may impact or impede subsequent steps in the investigation. For example, if the Google Order were revealed immediately, the government may be unable to obtain useful information from Google or other service providers in the future because the subjects of the investigation may alter their habits or simply destroy relevant information.

It is also important to note that revealing the existence of the Google Order might well disclose to subjects of the investigation additional information or clues about the speed, scope, and direction of the government's investigation, information the subjects could use to attempt to obstruct or frustrate the government's investigative efforts. Google counters that publication of the Google Order would result in only a trivial increase in the amount of information already publicly known about the WikiLeaks investigation. Were this argument adopted, the implications for future investigative actions by the government pursuant to the SCA would be dire. Google's argument, if followed to its logical end, would lead to the disclosure of every § 2703(d) order in the government's WikiLeaks investigation after a single initial public disclosure. Google's argument ignores this potential ripple effect. Therefore, even though the Twitter Order is already public, the government is correct in noting that disclosure of the Google Order may nonetheless further impede the WikiLeaks investigation.

In addition to concerns about the subjects of the investigation altering their behavior, the government also cites witness intimidation as a potential negative effect of unsealing the Google Order. In this regard, the government notes that the unsealing of the Twitter Order led to a wave of public criticism urging service providers to resist the government's requests for content and noncontent subscriber information. In the government's view, disclosure of the Google Order would further fuel this type of witness intimidation. Additionally, the government points out that service providers may face retribution for cooperating with the government in connection with SCA requests in the form of illegal attacks on the service providers' computer systems by supporters of WikiLeaks. The government notes that following disclosure of the Twitter Order, purported WikiLeaks supporters attacked the computer systems of various companies, including banks, that the supporters believed cooperated with the government's WikiLeaks investigation. This mode of witness intimidation, the government points out, would also be fueled by the disclosure of the Google Order. Given the events that occurred following disclosure of the Twitter Order, the government is correct to be concerned about the potential for increased witness intimidation that could result from disclosure of the Google Order. If the Google Order were unsealed, future service providers may do precisely what Google has done in this instance, namely resist compliance with a lawful § 2703(d) order by bringing baseless legal challenges that have the effect of impeding the government's progress in the WikiLeaks investigation.[9]

In sum, the government has persuasively demonstrated adequate and legitimate grounds for a court to conclude, as the magistrate judge did, that there is reason to believe that disclosure of the Google Order to the subscriber in question will seriously jeopardize the government's

---

[9] Given the reaction to the publication of the Twitter Order, it appears that the government may now regret consenting to disclosure of the Twitter Order.

ongoing investigation.[10] Thus, the magistrate judge's imposition of a ninety-day disclosure bar pursuant to § 2705(b) was neither clearly erroneous nor contrary to law. Nor does a *de novo* review of the record as a whole reveal any basis on which to modify the Google Order's nondisclosure provision. Therefore, under either standard of review, Google's objection in this regard must be overruled.

In addition to arguing that the government has failed as a factual matter to demonstrate that disclosure of the Google Order would seriously jeopardize the investigation, Google also asserts two legal grounds for rejecting the disclosure bar. First, Google contends that the order raises potential constitutional and statutory issues that an affected subscriber may wish to raise, but which cannot be raised at this time because the affected subscriber is unaware of the order's existence. The short answer to this argument is that if an individual whose information is sought by the Google Order wishes to attack the validity of the order, there will be opportunities for such a challenge after the order is made public. For example, if the information obtained is offered by the government in a subsequent criminal prosecution, a defendant with standing may seek exclusion of the evidence.[11] And of course, if no one is prosecuted based on the information obtained from Google, a § 1983 action might be available if the subscriber can demonstrate the requisite elements of the § 1983 action, including, most notably, a "deprivation

---

[10] The government also asserts that its investigation has been impeded following unsealing of the Twitter Order by diverting resources (i) to addressing public criticism of its investigatory tactics, and (ii) to defending its attorneys from harassment. The government contends that unsealing the Google Order would further exacerbate these conditions. The SCA does not include criticism of the government or harassment of government attorneys in the § 2705(b) calculus. Indeed, it is the integrity of the investigation itself, not the government's interests in protecting its image or defending its attorneys against harassment, that are the subject of § 2705(b).

[11] Of course, this is not to say that the defendant would have standing to challenge the admissibility of the evidence, or even that a defendant with standing could properly invoke the exclusionary rule in the circumstances. Those issues need not be and are not addressed here.

of any rights, privileges, or immunities secured by the Constitution and laws." 42 U.S.C. § 1983. Although it does not appear that a § 1983 action based on the Google Order would have any merit,[12] questions raised by such an action need not be addressed here.

Google's final objection to the Google Order's nondisclosure provision rests in the First Amendment. In essence, Google argues that the nondisclosure provision is an unlawful prior restraint on its own free speech rights inasmuch as the order prevents Google from discussing the existence of the order with anyone. Before addressing the merits of this argument, it is important to note initially that orders barring third parties from disclosing government surveillance tactics during the course of an investigation are hardly new. The government has long held the power to compel the assistance of, *inter alia*, telephone and internet service providers in monitoring communications. *See United States v. New York Tel. Co.*, 434 U.S. 159, 168 (1977) (recognizing the authority for the installation of a pen register); *United States v. Talbert*, 706 F.2d 464, 467 (4th Cir. 1983) (recognizing the authority for wiretaps); *see also* 18 U.S.C. § 3122 (authorizing statute for pen registers and trap and trace devices). Indeed, the statute invoked by the government here is nearly twenty five years old. *See* Electronic Communications Privacy Act of 1986, Pub. L. 99-508, § 201(a), 100 Stat. 1864, (1986). And when the government invokes its power to obtain information from service providers, courts routinely bar the providers from disclosing the existence of the order to anyone, including the relevant subscriber. *See, e.g.*, 18 U.S.C. § 3123(d) (barring disclosure of the existence of pen registers and trap and trace devices unless otherwise directed by a court); 18 U.S.C. § 2511(2)(a)(ii) (barring disclosure of the existence of wiretaps, unless otherwise directed by a court).

---

[12] *See In Re: §2703(d) Order*, Misc. No. 1:11dm00003, 2011 U.S. Dist. LEXIS 25322, at *10-19 (E.D. Va. Mar. 11, 2011) (Memorandum Opinion) (rejecting subscribers' First and Fourth Amendment challenges to the Twitter Order).

Google's First Amendment argument amounts to an as-applied attack on the SCA's constitutionality. Yet, Google cites no case—and none has been found—striking the exercise of such power as an improper prior restraint under the First Amendment. Nondisclosure provisions of this sort are so routine that Google's argument borders on frivolous. Nevertheless, it is not difficult to perform the required constitutional analysis under the First Amendment, which makes clear that the nondisclosure provision in the Google Order passes constitutional muster.

It is true, of course, that the nondisclosure provision in issue does constitute a prior restraint on Google's right to free speech,[13] but it is equally clear that a prior restraint is permissible where the government demonstrates that the restraint is narrowly tailored to serve a compelling governmental interest. *See Va. Dep't of State Police v. Wash. Post*, 386 F.3d 567, 573 (4th Cir. 2004) (analyzing prior restraints in the context of sealed court documents). It is well settled that the government has a compelling interest in maintaining the integrity of an ongoing criminal investigation. *Wash. Post*, 386 F.3d at 579 ("We note initially our complete agreement with the general principle that a compelling governmental interest exists in protecting the integrity of an ongoing law enforcement investigation."); *In re Sealing & Non-Disclosure*, 562 F. Supp. 2d at 895 ("As a rule, sealing and non-disclosure of electronic surveillance orders [that are not permanent or indefinite] are presumptively justified while the investigation is ongoing . . . ."). Of course, "whether this general interest is applicable in a given case will depend on the specific facts and circumstances presented." *Wash. Post*, 386 F.3d at 579. In conducting such an analysis, consideration must be given to "whether the granting of access . . . will disclose facts that are otherwise unknown to the public." *Id.*

---

[13] *See In re Sealing & Non-Disclosure*, 562 F. Supp. 2d 876, 882 (S.D. Tex. 2008) (noting that a nondisclosure provision in a § 1703(d) order "imposes a prior restraint on speech").

These principles, applied here, point convincingly to the conclusion that the nondisclosure provision in the Google Order does not infringe any of Google's First Amendment rights. Here, it is clear that unsealing the Google Order will reveal steps in the government's investigation that are not currently public. Although the public may speculate that the government is seeking or has sought access to noncontent subscriber information with respect to the [redacted] account, such access has ever been publicly confirmed. Moreover, as noted *infra*, there is reason to believe that such release will seriously jeopardize the government's ongoing criminal investigation. The government's interest in maintaining the integrity of its WikiLeaks investigation cannot be understated, and the temporary prior restraint on Google's free speech is narrowly tailored to serve this compelling interest. Therefore, Google's First Amendment challenge to the nondisclosure provision in the Google Order fails.

Accordingly, for the aforementioned reasons, the magistrate judge's order sealing the Google Order and barring disclosure of the existence of the Google Order for ninety days, with an optional sixty day extension, is neither clearly erroneous nor contrary to law. Additionally, a *de novo* review of the record similarly confirms that the magistrate judge's ruling was correct in all respects. Thus, Google's objections must be overruled.

The Clerk is directed to place this matter under seal and to send a copy of this Memorandum Opinion to all counsel of record.

Alexandria, Virginia
March 30, 2011

[redacted]
United States District Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

IN THE MATTER OF THE 2703(d) ORDER AND 2703(f) PRESERVATION REQUEST RELATING TO GMAIL ACCOUNT	)	**Misc. No. 1:10GJ3793**
	)	**11-DM-2**
	)	**UNDER SEAL**

ORDER

The matter is before the Court on Google, Inc.'s motion to stay and objections to the magistrate judge's ruling that the order issued to Google pursuant to 18 U.S.C. § 2703(d) remain under seal and that Google be ordered not to disclose the existence of the order to anyone. *See In re Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(d)*, No. 1:10GJ3793 (E.D. Va. Jan. 4, 2011) (Order), *as modified by In re 2703(d) Order and 2703(f) Preservation Request Relating to Gmail Account* [redacted] No. 1:10GJ3793 (E.D. Va. Feb. 9, 2011) (Order).

For the reasons stated in the accompanying Memorandum Opinion of even date, a *de novo* review of the record as a whole demonstrates that the magistrate judge's ruling is correct in all respects, and that the ruling is not contrary to law, clearly erroneous, or an abuse of discretion.

Accordingly,

It is hereby **ORDERED** that Google's objections (Doc. Nos. 15 and 16) are **OVERRULED** in all respects.

It is further **ORDERED** that Google's motion to stay (Doc. No. 17) is **DENIED AS MOOT.**

It is further **ORDERED** that this Order and the accompanying Memorandum Opinion shall **REMAIN UNDER SEAL** until further order of the Court.

It is further **ORDERED** that once the underlying grand jury investigation is completed, the government is **DIRECTED** to advise the Court whether it would then be appropriate to lift the seal on this Order and the Memorandum Opinion.

It is further **ORDERED** that Google promptly comply with the magistrate judge's § 2703(d) order compelling the disclosures described therein and comply with the accompanying nondisclosure provision in all respects.

The Clerk is directed to place this matter under seal and to send a copy of this Order to all counsel of record.

Alexandria, Virginia
March 30, 2011

[redacted]
United States District Judge

ATTACHMENT O

IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE 2703(D) ORDER AND 2703(F) PRESERVATION REQUEST RELATING TO GMAIL ACCOUNT	))))	Criminal No. 1:11-DM-2 UNDER SEAL

CONSENT MOTION TO UNSEAL

The United States of America and Google Inc. (Google) through undersigned counsel file this consent motion to unseal the redacted versions of the orders and pleadings in 1:11-DM-2 enclosed as Attachments A through O.

I. Background

On January 4, 2011, upon application of the United States pursuant to 18 U.S.C. §2703(d), Magistrate Judge [redacted] issued an order, requiring Google to disclose non-content subscriber and transactional records for a Google account. (Section 2703(d) Application; Section 2703(d) Order)

The Section 2703(d) Order provided that the "application and [ ] Order are sealed until otherwise ordered by the court, and that Google shall not disclose the existence of the application or [ ] Order . . . or the existence of the investigation to the listed subscriber or to any other person, unless and until authorized to do so by the Court. See *ex parte,* under seal Attachment. On February 9, 2011, Judge [redacted] denied in part and granted in part Google's Motion to Modify the Section 2703(d) Order. Google was authorized to provide notice of it to its subscriber within 90 days of providing the required information to the government, unless the government filed a motion for an extension, with a maximum sixty-day extension period. The clerk was directed to file the order under seal. ("Modified Disclosure and Sealing Order 1").

On March 30, 2011, Judge [redacted] overruled Google's objections to Judge [redacted] ruling, and ordered that the Order and accompanying Memorandum of Opinion remain under seal until further order of the Court. The United States was directed to advise whether it would be appropriate to lift the seal once the underlying grand jury investigation was completed. The clerk was directed to place the matter under seal. ("Modified Disclosure and Sealing Order 2"). On July 29, 2011, Google provided notice of the Section 2703(d) Order to the subscriber following expiration of the non-disclosure period.

II. Discussion

The Section 2703(d) Order and Section 2703(d) Application, which contains specific and sensitive details of the investigation, remain properly sealed while the grand jury investigation continues.

The United States believes, however, that alternatives less drastic than sealing will now suffice to protect the investigation with respect to the Modified Disclosure and Sealing Orders 1 and 2 and related pleadings in matter 1:11-DM-2 (except ex parte pleadings), which pertain to sealing and non-disclosure issues.

Specifically, the United States believes that those Orders and pleadings may be unsealed if "matters occurring before a grand jury" (i.e. accounts and individuals) and personal identifiers of government officials (i.e. names and contact information)[1] are redacted. The United States also will not seek to prevent Google from disclosing the account name at issue in matter 1:11-DM-2 to the subscriber of that account.

[1] The Attachments reflect redactions to the names and contact information of government and judicial officials. The United States and Google defer to the Court's preference in redacting the names of judicial officials.

III. Conclusion

Therefore, the United States and Google respectfully request that the following, redacted in accordance with Attachments A through O, be unsealed:

A. Google's Motion to Modify 2703(d) Order for Purpose of Providing Notice (1/18/11)

B. Government's Response (1/28/11)

C. Google's Reply (2/1/11)

D. Government's Motion to Continue (2/3/11)

E. Modified Disclosure and Sealing Order 1 (Judge [redacted]) (2/9/11)

F. Google's Objections to and Appeal of Judge [redacted] Order (2/17/11)

G. Google's Motion to Stay Production Pending Appeal (2/17/11)

H. Government's Response to Google's Objections (2/28/11)

I. Government's Response to Google's Motion to Stay (2/28/2011)

J. Google's Reply in Support of Objections (3/7/11)

K. Google's Reply in Support of Motion to Stay Production Pending Appeal (3/7/11)

L. Government's Notice of Relevant Decision (3/22/2011)

M. Google's Response to Notice of Relevant Decision (3/23/2011)

N. Modified Disclosure and Sealing Order 2 (Judge [redacted]) (3/30/11)

O. Redacted Consent Motion to Unseal and Order

Dated this 1st day of April 2015.

Respectfully submitted,

[redacted]

By:

[redacted]
Assistant United States Attorney
United States Attorney's Office
2100 Jamieson Avenue
Alexandria, Virginia 22314
Phone: (703) 299-3700
Fax: (703) 299-3980

Attorneys for the United States

_____
John K. Roche (VSB# 68594)
Perkins Coie LLP
700 13th St., N.W., Suite 600
Washington, D.C. 20005-3960
Phone: 202-434-1627
Fax: 202-654-9106
JRoche@perkinscoie.com

Attorneys for Google Inc.

CERTIFICATE OF SERVICE

I hereby certify that on this 1st day of April 2015 the foregoing was sent via email and hand deliver to the following persons:

John K. Roche
Perkins Coie LLP
700 13th St., N.W., Suite 600
Washington, D.C. 20005-3960
Phone: 202-434-1627
Fax: 202-654-9106
JRoche@perkinscoie.com

By: [redacted]
Assistant United States Attorney
United States Attorney's Office
2100 Jamieson Avenue
Alexandria, Virginia 22314
Phone: (703) 299-3700
Fax: (703) 299-3980

IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE 2703(D) ORDER AND 2703(F) PRESERVATION REQUEST RELATING TO GMAIL ACCOUNT	))))	Criminal No. 1:11-DM-2 UNDER SEAL

CONSENT ORDER

WHEREAS, the United States obtained a 2703(d) Order directed to Google Inc. (Google);

WHEREAS, the United States and Google engaged in litigation regarding the sealing and non-disclosure of the 2703(d) Order in the matter 1:11-DM-2; and

WHEREAS, based on the record before the Court, alternatives less drastic than sealing will now suffice to protect the investigation with respect to the documents specified below, which pertain to sealing and non-disclosure issues; it is hereby

ORDERED that the following, redacted in accordance with Attachments A through O, be unsealed:

A. Google's Motion to Modify 2703(d) Order for Purpose of Providing Notice (1/18/11)

B. Government's Response (1/28/11)

C. Google's Reply (2/1/11)

D. Government's Motion to Continue (2/3/11)

E. Modified Disclosure and Sealing Order 1 (Judge [redacted]) (2/9/11)

F. Google's Objections to and Appeal of Judge [redacted] Order (2/17/11)

G. Google's Motion to Stay Production Pending Appeal (2/17/11)

H. Government's Response to Google's Objections (2/28/11)

I. Government's Response to Google's Motion to Stay (2/28/2011)

J. Google's Reply in Support of Objections (3/7/11)

K. Google's Reply in Support of Motion to Stay Production Pending Appeal (3/7/11)

L. Government's Notice of Relevant Decision (3/22/2011)

M. Google's Response to Notice of Relevant Decision (3/23/2011)

N. Modified Disclosure and Sealing Order 2 (Judge [redacted]) (3/30/11)

O. Redacted Consent Motion to Unseal and Order

ORDERED that Google may disclose to the subscriber the account at issue in the sealing and non-disclosure litigation relating to 1:11-DM-2, and the subscriber is not prohibited from further disclosing that information.

ORDERED the record in matters 1:11-DM-2 remain under seal, and no part of them may be disclosed without court order except to the extent provided above.

It is so ORDERED.

ENTERED this __ day of April 2015, at Alexandria, Virginia.

_____