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. 10GJ3793 1:11-DM-00003

OBJECTIONS OF REAL PARTIES IN INTEREST JACOB APPELBAUM, BIRGITTA JONSDOTTIR AND ROP GONGGRIJP TO MARCH 11, 2011 ORDER DENYING MOTION TO VACATE AND DENYING IN PART MOTION TO UNSEAL

TABLE OF CONTENTS

Page

Federal Cases

Federal Statutes

Federal Rules

Constitutional Provisions

Other Authorities

I. INTRODUCTION

Real parties in interest Jacob Appelbaum, Birgitta Jonsdottir, and Rop Gonggrijp (the "Parties") hereby submit their objections to Magistrate Judge Buchanan's March 11, 2011 Order (Dkt. No. 39) denying the Parties' Motion to Vacate a December 14, 2010 Order requiring Twitter, Inc. to disclose information related to the Parties' private Twitter accounts, and denying in part the Parties' Motion for Unsealing of Court Records ("Magistrate's Order").

The Magistrate's Order should be overturned, and the December 14 Twitter Order should be vacated, because the Twitter Order violates the Stored Communications Act ("SCA"), intrudes upon the Parties' First Amendment freedoms of speech and association, and threatens the Parties' Fourth Amendment rights to privacy. The Court should also unseal all documents relating to the Twitter Order, and any similar orders to other entities under the SCA, because the government has not met its burden of demonstrating a compelling interest in secrecy that heavily outweighs the significant interests of the Parties and the public in accessing these documents.

II. FACTUAL AND PROCEDURAL BACKGROUND[1]

A. Twitter

Twitter is an online micropublishing tool that permits individuals to communicate with others around the world, on any subject, in messages of 140 characters or less. Twitter is one of the fastest growing forms of communication in the world, with over 175 million registered users as of September 2010.[2] Twitter has been an especially vital form of communication for individuals who either do not have access to more traditional media or who live in repressive

[1] The Parties' original Motion to Vacate and Motion for Unsealing contained more detailed discussions of the factual and procedural background. *See* Dkt. Nos. 1, 3. Due to space constraints, the Parties provide a limited discussion here, but incorporate their original pleadings by reference.

[2] Eric Schoenfeld, *How Big is Twitter Really?*, TechCrunch.com, April 16, 2010, *available at* http://techcrunch.com/2010/04/16/how-big-twitter/; *see also* Pew Internet & American Life Project, Twitter and Status Updating, Fall 2009 (Oct. 2009), *available at* http://www.pewinternet.org/~/media//Files/Reports/2009/PIP_Twitter_Fall_2009web.pdf.

societies without freedom of speech, such as Egypt, Tunisia, and Iran.[3] Twitter thus enables any individual to "become a town crier with a voice that resonates farther than it could from any soapbox." *See Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 870 (1997).

To publish on Twitter, an individual must sign up for a Twitter account. A subscriber can then publish messages ("Tweets"), sign up to receive others' Tweets, and have others follow his or her Tweets (one's "followers"). While a Tweet's content, time, and date appear publicly, the location from where the Tweet was made—available from the Internet Protocol (IP) address[4] of the speaker—does not. Nor does the Tweet reveal the other online locations that a person has visited during that session, something IP addresses may also reveal. Besides public Tweets, users may also communicate privately with other Twitter users via direct messages ("DMs"). The content, sender, recipient, date, and time of DMs are not publicly available.

Here, all three Parties have public Twitter feeds through which they express opinions on public issues. Birgitta Jonsdottir is an elected Member of the Parliament of Iceland, who uses Twitter to communicate on a variety of topics including her political positions, activities, and work as a Member of Parliament. Jacob Appelbaum is a U.S. citizen and a well-known computer and telecommunications security researcher, who regularly uses Twitter to tweet about matters of public concern such as Internet censorship, human rights issues, Internet security, and other political and social issues. Rop Gonggrijp is a Dutch activist and businessman who is an expert in computer and telecommunications security and who uses Twitter to post public

---

[3] Ethan Zuckerman, *The First Twitter Revolution?*, Foreign Policy, January 14, 2011, *available at* http://www.foreignpolicy.com/articles/2011/01/14/the_first_twitter_revolution?page=full; *see also* Brad Stone & Noam Cohen, *Social Networks Spread Defiance Online,* N.Y. Times, June 16, 2009, at A11, *available at* http://www.nytimes.com/2009/06/16/world/middleeast/16media.html.

[4] An Internet Protocol ("IP") address is a unique numerical address that identifies individual computers or other devices as they interact over the Internet. IP addresses can be used to determine where a computer is located when it is connected to the Internet and to track Internet users across multiple online services, since the IP address usually remains the same for each session (or even over multiple sessions) as the user moves from one online service to another.

messages through his blog, http://rop.gonggri.jp/.

B. The Order Requiring Twitter's Disclosure of Extensive Information

In response to an *ex parte* Application by the United States ("Application"), the Magistrate issued an Order on December 14, 2010 that requires Twitter to disclose information concerning several Twitter accounts, @wikileaks, @ioerror, @birgittaj, and @rop_g—the last three of which are held by the Parties. *See* Declaration of Stuart Sears in Support of Objections ("Sears Decl."), Ex. 1.[5] Among other things, the Twitter Order requires Twitter to disclose the Parties': (1) personal contact information, including addresses, (2) financial data, including credit card or bank account numbers, (3) account activity information, including the "date, time, length, and method of connections" and the "source and destination Internet Protocol address(es)," and (4) DM information, including the email addresses and IP addresses of everyone with whom the Parties have had DMs. *See id.* The Twitter Order seeks all activity on the accounts, apparently including DMs, regardless of subject matter, for the time period from November 1, 2009 to the present.[6]

The Twitter Order requires disclosure of non-public information about all of the Parties' Twitter-related speech for multiple months (originally over one year) regardless of any connection to WikiLeaks (the apparent subject of the investigation). Such information is also requested for all of the Parties' Twitter-based DMs during this period—again, regardless of any

[5] Unless otherwise noted, all exhibits cited herein are attached to the Sears Declaration, submitted herewith.

[6] The Parties understand the government is currently restricting the scope of the information sought, including the time period to November 15, 2009 through June 1, 2010. Nonetheless, the Magistrate upheld the original Twitter Order, and the government has not conceded that the Order is improper, nor has it agreed to give up its ability to later seek the full scope of information sought by the Twitter Order. As a result, the Parties' challenge to the Twitter Order is not limited to the government's presently narrowed demand. *See Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 189 (2000) ("Voluntary cessation of a challenged practice does not deprive a federal court of its power to determine the legality of the practice.") (citation omitted).

connection between the messages and WikiLeaks. The Twitter Order's breadth is especially significant because the Parties use Twitter extensively and/or have thousands of "followers" who follow what they post,[7] and each publishes many Twitter messages wholly unrelated to WikiLeaks, including Tweets discussing Tibet and Tunisia, the Icelandic volcano, the Transportation Security Administration, obscenity, and gay marriage laws. Ex. 2.

The Twitter Order was issued pursuant to 18 U.S.C. § 2703(d), a part of the SCA. Ex. 1. To obtain a § 2703(d)order, the government must offer "specific and articulable facts showing that there are reasonable grounds to believe" that the information or records sought are both "relevant and material to an ongoing criminal investigation."

While the SCA does not explicitly provide for the sealing of orders issued pursuant to its terms,[8] the Twitter Order and related documents were sealed, and the Order prohibited Twitter from disclosing it. The government subsequently moved to unseal the Order; on January 5, 2011, the Court found that unsealing was "in the best interest of the investigation" and unsealed the Twitter Order, but not the underlying Application or any related documents (the "Unsealing Order"). Ex. 3.

On January 7, 2011, Twitter informed the Parties of the Twitter Order, advising them that Twitter would be forced to comply with it unless the Parties took appropriate legal actions.

---

[7] As of January 25, 2011, the time of the Parties' filing of the Motion to Vacate the Twitter Order, Mr. Appelbaum had posted 7,909 Tweets and had 10,699 followers, Ms. Jonsdottir had posted 1,211 Tweets and had 5,904 followers, and Mr. Gonggrijp had posted 77 Tweets and had 4,223 followers.

[8] Prior notice to the affected subscriber is not statutorily required if the government uses a warrant or only seeks disclosure of "a record or other information pertaining to a subscriber to or customer of [an electronic communication or remote computing] service," although it is required where a court order is used to seek the "contents" of any electronic communication. 18 U.S.C. §§ 2703(b), (c). Where the government is not required to provide notice or is entitled to delay notice, the government may also obtain a court order commanding the communications provider not to notify anyone of the existence of the warrant, subpoena, or court order "for such period as the court deems appropriate," provided that the court determines that notification "will result in" a specifically defined adverse result. *Id.* § 2705(b).

Ex. 4. The disclosure of the Twitter Order was front-page news around the world.[9] Widespread interest has focused on whether similar orders have been issued to other companies concerning the Parties.[10] Other companies believed to have received similar orders have refused to comment.[11]

C. The Magistrate's March 11, 2011 Order Denying the Parties' Motion to Vacate and Motion to Unseal

On January 26, 2011, the Parties filed a Motion to Vacate the Twitter Order and a Motion for Unsealing of Court Records, including any § 2703 orders to companies other than Twitter regarding the Parties.[12] Dkt. Nos. 1-4. Following oral argument, on March 11, 2011, the Magistrate denied the Parties' Motion to Vacate, and denied in part the Parties' Motion for Unsealing. Ex. 5 (Memorandum Opinion) (hereinafter "Op.").

III. ARGUMENT

A. The Standard of Review is De Novo.

The Parties submit their objections to the Magistrate Order under Federal Rule of Criminal Procedure 59 or Federal Rule of Civil Procedure 72, which require *de novo* review since resolution of this Order is dispositive as to the Parties' claims. *See ALCOA v. U.S. Envtl. Prot. Agency*, 663 F.2d 499, 501-502 (4th Cir. 1981).

---

[9] *See, e.g.*, Scott Shane & 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.

[10] *See, e.g.*, Barton Gellman, *Twitter, Wikileaks and the Broken Market for Consumer Privacy*, Time Magazine: Techland, Jan. 14, 2011, *available at* http://techland.time.com/2011/01/14/twitter-wikileaks-and-the-broken-market-for-consumer-privacy/.

[11] *See, e.g.*, *id.*; Miguel Helft & Claire Cain Miller, *1986 Privacy Law Is Outrun by the Web*, N.Y. Times, Jan. 10, 2011, at A1, *available at* http://www.nytimes.com/2011/01/10/technology/10privacy.html

[12] To the extent that these other orders and related documents are filed under a separate docket number, the Parties respectfully requested that a copy of their Motion for Unsealing be filed in the correct docket(s).

B. The Magistrate's Decision on the Parties' Motion to Vacate the Twitter Order Should Be Rejected.

1. The Parties have Standing to Challenge the Twitter Order.

The Magistrate improperly relied on an irrelevant section, §2704(b)(1)(A) of the SCA, to deny the Parties standing on their motion to vacate. This statutory analysis is wrong and raises due process concerns because it renders an individual powerless to prevent even a plainly illegal disclosure of his information to the government.

Section 2704(b)(1)(A) is not a freestanding section. It is a subsection of § 2704, entitled "Backup Preservation," a separate part of the SCA that is not at issue here. Section 2704(a)(1) allows the government to compel a service provider to create a backup copy of the contents of electronic communications and requires notice to the subscriber under § 2704(a)(2). Section 2704(b) allows a subscriber who has received the required notice of a backup preservation order under § 2704(a)(2) to challenge it. A challenge must be brought "within fourteen days after notice by the governmental entity to the subscriber or customer under subsection (a)(2) of this section." 18 U.S.C. § 2704(b). By its terms, therefore, § 2704(b)(1)(A) only applies to challenges brought to orders issued under § 2704(a). It has no bearing on challenges to orders under § 2703, such as the Parties' challenge.

Further, the Magistrate's finding that § 2704 "seems" to recognize that only targets of a content disclosure "would have a viable constitutional challenge" flouts the SCA's plain language and established law.[13] As noted above, § 2704 is limited to a backup preservation order. Moreover, courts have long recognized a right to challenge disclosure demands that raise constitutional issues. *See Eastland v. U.S. Servicemen's Fund*, 421 U.S. 491, 501 n.14 (1975). The Magistrate acknowledged that disclosure orders under the SCA "resemble subpoenas," but failed to address this authority. Op. at 9 n.4. There is no basis in the statute to distinguish

[13] Any remedies or judicial sanctions provided for in the SCA are explicitly limited to "non-constitutional" violations. *See* 18 U.S.C. § 2708.

between standing to challenge orders that seek content and orders that do not.[14]

Nor is there any support for the Magistrate's finding that, even when a subscriber is not entitled to notice under the SCA, she lacks standing to challenge an order of which she becomes aware. Here, of course, the Magistrate determined that the provider could give notice. The SCA requires the government to show that the information it seeks is "relevant and material to an ongoing criminal investigation." *See* 18 U.S.C. § 2703(d). To construe the SCA as precluding an adversarial challenge by the person affected by the disclosure, would essentially read those limitations out of the statute and render a court's decision to give notice, as here, an empty gesture. The Supreme Court long ago held that the fact that a statute may tolerate the disclosure of certain records without requiring notice does not preclude a party's challenge if it receives notice. *See, e.g.*, *Eastland*, 421 U.S. at 501 n.14.

Finally, the Parties have standing to challenge the Twitter Order for both its statutory and constitutional transgressions because the foundation of our legal system is an adversarial process that ensures that persons whose rights are affected have the opportunity to challenge government action. As Justice Frankfurter long ago cautioned, "democracy implies respect of the elementary rights of men . . . [and] must therefore practice fairness; and fairness can rarely be obtained by secret, one-sided determination of facts decisive of rights." *Joint Anti-Fascist Refugee Committee v. McGrath*, 341 U.S. 123, 170 (1951) (Frankfurter, J., concurring). Fundamental fairness and due process demand that the Parties have the right to challenge disclosure of their records here. *See Rafeedie v. INS*, 880 F.2d 506, 524-25 (D.C. Cir. 1989) (applying due process balancing test for exclusion proceedings and use of secret evidence, emphasizing that "the fundamental requirement of due process is the opportunity to be heard 'at a meaningful time and in a meaningful manner'") (quoting *Matthews v. Eldridge*, 424 U.S. 319, 333 (1976).

[14] Moreover, the SCA does not identify or contemplate the disclosure of IP addresses recorded over a period of time. *See* Op. at 4-5 (listing "records" under the SCA). Especially where IP addresses can reveal the location and movements of an individual, the government's request for

2. The Twitter Order Violates § 2703 of the SCA.

The Magistrate next erred in finding that the Twitter Order satisfied the SCA's standard that an order for disclosure may issue "only if" the government provides "specific and articulable facts showing that there are reasonable ground to believe that the . . . records or information sought[ ] are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

Section 2703's "specific and articulable facts" standard requires more than mere suspicion. Even to justify 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); *United States v. Brignoni-Ponce*, 422 US 873, 882, 884-85 (1975) (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, the government is not merely engaging in a brief investigative stop, but is seeking non-public information about the Parties' protected Twitter-based speech and associational contacts over an extended period of time. And yet the government's Application appears to be based directly on an "unparticularized suspicion or hunch" that all of the Parties' Twitter records have some connection to its WikiLeaks investigation. This cannot be the case—the vast majority of the Parties' Twitter activity has nothing to do with WikiLeaks. *See supra* at 2, 3-4. At a minimum, the government must be required to articulate "specific and articulable facts" that do more than speculate about a nexus between the information sought and the investigation's potential targets.

Moreover, the Magistrate ignored § 2703's materiality element. *See* Op. at 7 (claiming that § 2703 is "routinely used to compel disclosure of records, only some of which are later determined to be essential to the government's case"). In a number of contexts, the United States

---

IP address information may not properly constitute a mere records disclosure.

Supreme Court and the Fourth Circuit have emphasized that a showing of materiality requires more than theoretical relevance. To establish materiality, the government must establish through more than mere speculation that the information is "vital" or "highly relevant" to the inquiry or "helpful" or "essential" to its 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). Especially since individuals typically do not receive notice of such orders, the government cannot be permitted to blindly request everything that "might" be useful and ignore § 2703's materiality requirement.

3. This Court Has the Discretion to Vacate the Order and Must Do So To Avoid the Constitutional Questions that It Raises.

As recently recognized by the Third Circuit, 18 U.S.C. § 2703(d) gives courts the discretion to deny applications for orders under that section—and, by extension, the discretion to vacate such orders—even when the government has successfully made the requisite factual showing. *See In re Appl. of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304, 315-17, 319 (3d Cir. 2010) ("*Third Circuit Opinion*").[15] Under the doctrine of constitutional avoidance, courts must avoid unnecessarily answering serious constitutional questions. *See Ashwander v. Tennessee Valley Auth.*, 297 U.S. 298, 346-48 (1936) (Brandeis, J., concurring). As set forth in the following sections, the Twitter Order here raises serious First and Fourth Amendment questions; as such, this Court can and must use the discretion granted to it by Congress and vacate the Twitter Order.[16]

---

[15] As *Third Circuit Opinion* explains, Congress provided this discretion 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 the issuance of a § 2703(d) order. *Id.* at 315-17. Accordingly, courts have the discretion to require the government to proceed by obtaining a search warrant based on probable cause, issued under Federal Rule of Criminal Procedure 41 pursuant to 18 U.S.C. § 2703(c)(1)(a). *See id.* at 316, 319.

[16] The Magistrate, in declining to exercise her own discretion, opined that requiring a showing of

4. The Twitter Order Violates the Parties' First Amendment Rights of Speech and Association.[17]

The Twitter Order seeks detailed information about the Parties' communications, including how often the Parties used Twitter to express themselves and to view what others had to say, when the Parties used Twitter, and where they were at all such times over an extended period of time. It seeks IP addresses that can track their use of other publishing services online. It also seeks information about the identity and geographical location of every person with whom the Parties have associated by exchanging private DMs. Contrary to the Magistrate's conclusion that there is nevertheless no chilling effect because the Parties "have already made their Twitter posts and associations publicly available," Op. at 9, none of this requested information—in particular, their "associations"—is publicly available. It is all private. The Twitter Order thus

---

probable cause would needlessly hamper an investigation, citing *In re Subpoena Duces Tecum*, 228 F.3d 341, 348-49 (4th Cir. 2000). *See* Op. at 7. Yet the *In re Subpoena* Court relied heavily on the fact that a subpoena "commences an adversary process during which the person served with the subpoena may challenge it in court ...." *Id.* at 348. Here, it would be especially unfair to deny the Parties any adversarial process under § 2703, as the Magistrate did through the erroneous standing ruling, while refusing to hold the government to the higher probable cause standard.

[17]The Magistrate expressed "serious doubts" that Ms. Jonsdottir and Mr. Gonggrijp "enjoy rights under the U.S. Constitution," because they are non-citizens residing abroad. Op. at 8 n.1 (citing *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990), and *Wang v. Reno*, 81 F.3d 808 (9th Cir. 1996)). These doubts are misplaced. *Verdugo-Urquidez* addresses only extraterritorial searches and seizures. *See, e.g.*, *United States v. Wanigasinghe*, 545 F.3d 595, 597 (7th Cir. 2008); *Lamont v. Woods*, 948 F.2d 825, 834 (2d Cir. 1991). Here, the Twitter Order was issued by a United States Magistrate and directed at information stored in the United States; hence, the Constitution governs the order, and *Verdugo* is inapplicable. Moreover, *Wang*—far from casting "doubts" on the rights of Ms. Jonsdottir and Mr. Gonggrijp—confirms that the First and Fourth Amendments apply here. In *Wang*, the Ninth Circuit rejected the government's argument based on *Verdugo* that a foreign individual could not assert a due process violation arising from government actions taken within the United States because those actions had occurred when the individual was not present here. Focusing on where the government conduct took place, the court found that those actions violated the Constitution. 81 F.3d at 817-20 & n.16. Similarly, the Second Circuit in *Lamont* contrasted the government's conduct in *Verdugo*, which "occurred solely in Mexico," with the alleged Establishment Clause violation alleged in *Lamont*, which would have occurred "in the United States." 948 F.2d at 834. Because the government's action here occurred entirely within the United States, Ms. Jonsdottir and Mr. Gonggrijp may invoke the protections of the First and Fourth Amendments.

has a chilling effect not only on the Parties' speech and association rights, but on the rights of Twitter users in general, including the Parties' followers, who will now fear that the government may secretly track their activities, seize their account information, and even map their movements and associations based on what they say about matters of public concern or with whom they communicate regarding political issues.[18] As the Supreme Court has cautioned, "[t]hese freedoms are delicate and vulnerable, as well as supremely precious in our society." *NAACP v. Button*, 371 U.S. 415, 433 (1963). Thus, "[t]he threat of sanctions may deter their exercise almost as potently as the actual application of sanctions." *Id.*

Contrary to the Magistrate's finding that the Twitter Order should stand because it supposedly does not seek to control or direct the contents of the Parties' speech, any governmental efforts that have the effect of chilling expression must withstand First Amendment scrutiny. *N.C. Right To Life v. Bartlett*, 168 F.3d 705, 715 (4th Cir. 1999). Where, as here, "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 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 Nat'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.").[19] As the Supreme Court has cautioned,

---

[18] The Parties have standing to raise the First Amendment rights of those not before the Court. *See, e.g.*, *Broadrick v. Oklahoma*, 413 U.S. 601, 612 (1973).

[19] 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*

"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).

The Twitter Order collides directly with the Parties' First Amendment rights, by among other things, requiring private IP address information and other details for all the Parties' Twitter messages posted over a period of more than six months. It is undisputed that most of these postings and messages have nothing to do with WikiLeaks. *See supra* at 3-4. That is not permissible. *See, e.g.*, *Button*, 371 U.S. at 433 ("Because First Amendment freedoms need breathing space to survive, government may regulate in the area only with narrow specificity."). The Magistrate, thus, failed to evaluate this intrusive demand with the requisite scrutiny.

The Magistrate Order also erroneously found "no cognizable First Amendment violation" because the Twitter Order "is a routine compelled disclosure of non-content information which petitioners voluntarily provided to Twitter pursuant to Twitter's privacy policy." Op. at 9. Whether this information was voluntarily provided to Twitter (which it was not) does not eliminate or lessen the Parties' First Amendment rights. *See, e.g.*, *In re First Nat'l Bank*, 701 F.2d at 118 ("[T]he constitutionally protected right, freedom to associate freely and anonymously, will be chilled equally whether the associational information is compelled from the organization itself or from third parties."). Nor does the ostensibly routine nature of the demand matter; to the contrary, if the government is routinely asking courts to issue overbroad demands for information about individuals' lawful Internet communications, that makes it all the more important for this Court to make clear that such demands are not permissible.

Finally, in finding that the "Twitter Order does not seek to control or direct the contents

---

87-3 Subpoena, 955 F.2d 229, 232-34 (4th Cir. 1992). But in that case, the interested party's First Amendment rights were not implicated, so the Court avoided the substantial relationship test issue. *Id.* 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. *Id.* at 234.

of petitioner's speech," the Magistrate sidestepped the reason that the government chose to seek information from Twitter—it is a publishing service that the Parties used to discuss Wikileaks. *See* Op. at 9. While the government has refused to provide the Parties with its Application, it 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."[20] No matter how much the government dislikes any given speech or advocacy, it cannot use that protected conduct as a pretext for overbroad searches or a basis for criminality.

The Court should vacate the Twitter Order in light of these First Amendment principles. Unless the government can show that the specific information sought bears a substantial relation to an overriding and compelling state interest, the government's efforts to seek private data regarding the Parties' Twitter use should be rejected.

5. The Twitter Order Violates the Parties' Fourth Amendment Privacy Rights.

The Parties have a reasonable expectation of privacy in the IP addresses they used at particular dates and times when logging into their Twitter accounts, because that information can be used to track the Parties' locations in, and movements between, particular private spaces over a period of time. *See United States v. Karo*, 468 U.S. 705, 707, 714-16 (1984) (holding that location tracking "falls within the ambit of the Fourth Amendment when it reveals information that could not have been obtained through visual surveillance"). As the Second Circuit explained, "[e]very 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) . . . ." *Register.com, Inc. v. Verio, Inc.*, 356 F. 3d 393, 409 (2d Cir. 2004) (citation omitted). In many instances, this information can then easily be

[20] *See* Pete Yost, Assoc. Press, *Holder says Wikileaks under investigation*, Nov. 29, 2010, *available at* http://news.yahoo.com/s/ap/20101129/ap_on_go_ca_st_pe/us_wikileaks_holder.

translated into the physical location of the computer user, based on publicly available information. As one court observed, IP addresses can be matched up with specific geographic designations using a publicly-available database operated by the American Registry for Internet Numbers, which "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 a particular IP address does not reveal a precise physical location, an IP address in combination with the records of the Internet Service Provider that assigned it can.[21]

The conclusion that the IP address information demanded by the Twitter Order is protected by the Fourth Amendment is further bolstered by the D.C. Circuit's recent holding that warrantless use of a GPS device to track the movements of an individual's car over the course of one month violates the Fourth Amendment. *United States v. Maynard*, 615 F.3d 544, 559 (D.C. Cir. 2010). As that court explained, even though a 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; *see also Third Circuit Opinion*, 620 F.3d at 312 ("If [cell site location information ("CSLI")] can be used to allow the inference of present, or even future, location [of a person], 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* to the extent it reveals the person's location in a private space). Similarly, IP address information can reveal an "intimate picture" of the Parties' movements between the private spaces from which they use Twitter. *See id.*

Contrary to the Magistrate's finding, this IP address information was not "voluntarily

[21] 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, a*vailable at*

conveyed" to Twitter like the bank records in *United States v. Miller*, 425 U.S. 435 (1976), or the dialed phone numbers in *Smith v. Maryland*, 442 U.S. 735 (1979), both of which the Supreme Court found were not protected by the Fourth Amendment. *See* Op. at 11. In both *Miller* and *Smith*, the relevant financial documents and dialed numbers were directly, visibly and knowingly conveyed to bank tellers and telephone operators or their automated equivalents. *See, e.g.*, *Smith*, 442 U.S. at 744. The phone customer knew and saw what numbers he was exposing to the phone company, and the bank customer knew and saw what documents he was exposing to the bank.

In contrast, the Twitter IP log information at issue here is passively communicated without any action by, knowledge of, or visibility to, the user. The user does not "dial" or type in her IP address; her web browser does not show her that address or indicate that it is being transmitted. Such automatic, passive, and largely hidden exposure of IP information to a service provider like Twitter is nothing like the direct, visible conveyance of phone numbers to an operator or bank documents to a teller. Indeed, the Internet user's situation as to an IP address is more like that of a cell phone user as to CSLI: when a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed is the number that is dialed, and there is no indication to the user that location information is also being revealed. *See Third Circuit Opinion*, 620 F.3d at 317-18 (distinguishing *Smith* and *Miller* and holding that CSLI is not voluntarily conveyed). The IP logs sought here are equally distinguishable from the information at issue in *Miller* and *Smith* and are analogous to the CSLI at issue in the *Third Circuit Opinion.*

The other cases relied on by the Magistrate to conclude that IP addresses are "voluntarily conveyed" and thus unprotected are inapposite. In particular, *United States v. Bynum*, 604 F.3d 161 (4th Cir. 2010), is wholly off point. It concerned only "basic subscriber" information that was obviously and affirmatively conveyed by the user to his internet and telephone service

---

http://www.justice.gov/criminal/cybercrime/ssmanual/ssmanual2009.pdf.

providers, "i.e., his name, email address, telephone number, and physical address." *Id.* at 164, and explicitly did not rule on the Fourth Amendment status of IP addresses, *id.* at 164 n.2. Similarly, the glancing analysis in *United States v. Perrine*, 518 F.3d 1196 (10th Cir. 2008), dealt only with "subscriber information provided to an internet provider" such as "name [and] address" and did not address IP addresses. *Id.* at 1204. Such basic subscriber information is not analogous to a passively exposed IP address of which the user may have no awareness.

The Magistrate was also mistaken to rely on a case holding that Internet "pen register" surveillance that captures the IP addresses connected to a target's computer does not implicate the Fourth Amendment. *See United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008). That case is distinguishable. Unlike in *Forrester*, where IP addressing information was used by the target's Internet Service Provider to route his communications and therefore was arguably analogous to dialing information, Twitter's IP logs serve no such purpose. Also, unlike the information at issue in *Forrester*, the IP information held by Twitter is "merely passively conveyed through third party equipment" and not "voluntarily turned over to direct the third party's servers" as in *Forrester*. *See id.* at 510. Furthermore, the information at issue in *Forrester*—the IP addresses of web sites that a target visited using his home computer, as opposed to the IP logs of the sites that a person visited from multiple IP addresses—did not implicate locational privacy. The logs in *Forrester* revealed only where a target was going in cyberspace; the logs at issue here reveal the Parties' real-world movements.[22]

The Magistrate also erroneously concluded that Twitter users "voluntarily convey[] their IP addresses to Twitter as a condition of use" based on her assumption that, "[b]efore creating a Twitter account, readers are notified that IP addresses are among the kinds of "Log Data" that

[22] Additionally, *Forrester* was wrongly decided because it failed to grapple with the same issue that was dispositive in the *Third Circuit Opinion*—that Internet users, like cell phone users and their CSLI, do not voluntarily or knowingly take any action to disclose information about their IP addresses when they use the Internet.

Twitter collects, transfers and manipulates." Op. at 13-14. First, the Magistrate inaccurately assumed that users who sign up for Twitter accounts are explicitly notified, before they create a Twitter account, that IP addresses are collected. This is not correct—nothing in the Twitter web pages, or Terms and Conditions, that are immediately apparent to users when they sign up for an account discuss IP addresses or the collection of Log Data.[23] Additionally, nothing in these pages clearly and explicitly directs users to review Twitter's Privacy Policy before creating an account.[24] Moreover, research shows that many Internet users do not read the privacy policies for the Internet sites they visit, so it is doubtful that Twitter users would have read such policies, much less understood them. *See* Dkt. No. 30 at 14 n.8. Second, the mere fact that Twitter has a privacy policy that, if accessed and read, notifies its customers that Twitter may also access certain information is not dispositive. For example, email users understand that their email provider stores copies of their messages, and may be subject to service or privacy policies stating that the provider may access that content in the ordinary course of business. Yet the Sixth Circuit had no difficulty concluding that email users nevertheless maintain an expectation of privacy in their emails. *United States v. Warshak*, 631 F.3d 266, 286-88 (6th Cir. 2010); *see also United States v. Heckenkamp*, 482 F.3d 1142, 1146-47 (9th Cir. 2007) (holding that a student did not lose his reasonable expectation of privacy in information stored on his computer, despite a university policy that it could access his computer while it was connected to the university's network). The same is true here; the mere fact that Twitter has access to the information does not eliminate the expectation of privacy in it.

---

[23] *See* Declaration of Karen Bringola, Ex. 1, submitted herewith.

[24] Instead, a user must notice the reference to Twitter's Privacy Policy, decide to click on the policy, and read the multi-page document to learn that IP addresses "may" be collected. *Id.*, Ex. 3. However, this policy also states that user's "location information" will not be collected unless they specifically allow this to occur. *Id.*

C. The Magistrate Erred in Denying the Motion to Unseal Because the Government Has Not Met its Heavy Burden to Keep the Court Records Sealed.

There is a presumption of access to judicial records and documents enshrined in both the common law and the Constitution. *Nixon v. Warner Commc'ns, Inc.*, 435 U.S. 589, 597 (1978); *Va. Dep't of State Police v. Wash. Post*, 386 F.3d 567, 575 (4th Cir. 2004). The public's interest in access may be magnified "[i]n the context of the criminal justice system" because "[s]ociety has an understandable interest not only in the administration of criminal trials, but also in law enforcement systems and how well they work." *In re Application & Affidavit for a Search Warrant*, 923 F.2d 324, 330-31 (4th Cir. 1991). "Regardless of whether the right of access arises from the First Amendment or the common law, it 'may be abrogated only in unusual circumstances.'" *Va. Dep't of State Police*, 386 F.3d at 576 (quoting *Stone v. Univ. of Md. Med. Sys. Corp.*, 855 F.2d 178, 182 (4th Cir. 1988)).

As described below, no such circumstances exist here. The Magistrate erred in denying the Motion to Unseal.

1. The Magistrate Applied The Wrong Legal Tests.

The Magistrate applied the wrong legal tests to both the common law and constitutional rights of access. First, the Magistrate erroneously concluded that the common law presumption of access to judicial records "may be overcome by a countervailing government interest." Op. at 18. That is not correct. The government must demonstrate that its "countervailing interests heavily outweigh the public interests in access." *Va. Dep't of State Police*, 386 F.3d at 575 (quotation omitted) (emphasis added).

Second, the Magistrate also applied the wrong test in determining that there was no First Amendment right of access. According to the Magistrate, the First Amendment right attaches "only when" the two conditions of experience and logic are each satisfied. *See* Op. at 18-19. The Supreme Court, however, identified "experience and logic" as "complementary considerations" for determining if there is a First Amendment right of access, not dispositive

elements that must always be present. *Press-Enterprise Co. v. Superior Court*, 478 U.S. 1, 8 (1986). Where, as here, there is not a centuries-old history of openness upon which to draw because the type of proceeding at issue is relatively new, courts have focused on the "logic" prong. Otherwise, the right of access would be limited to processes that existed in a prior era. Thus, in *Press-Enterprise*, the Supreme Court held that the First Amendment right attached to pretrial proceedings even though they had "no historical counterpart," where the "importance of the . . . proceeding"—the logic prong—was clear. *Id.* at 11 n.3.[25]

The Magistrate failed to undertake a proper "logic" analysis, which involves examining whether access would play a "significant positive role in the functioning of the particular process in question." *Id.* at 8-9. Instead, the Magistrate focused exclusively on the government's purported need for secrecy and ignored the positive role that openness regarding § 2703 proceedings would serve. Op. at 19. Had the Magistrate conducted the proper analysis, it would have been clear that openness would aid the § 2703 process for the same reason that courts have deemed the First Amendment and common law rights of access to apply to most court proceedings: transparency ensures fairness, decreases bias, improves public perception of the justice system, and enhances the chances that orders are well-justified and not overbroad. *See, e.g.*, *Nixon,* 435 U.S. at 598 (judicial transparency serves "the citizen's desire to keep a watchful eye on the workings of public agencies . . . [and] the operation of government."); *United States v. Moussaoui*, 65 F. App'x 881, 885 (4th Cir. 2003) ("The value of openness in judicial proceedings can hardly be overestimated."). Indeed, had the Twitter Order not been unsealed, the Parties and the public would never have known its breadth, and they would have been unable to mount a challenge to protect their constitutional rights. Because unsealing these documents would have a significant, positive impact on the judicial process under § 2703, there is a First

[25] *See also United States v. Gonzales*, 150 F.3d 1246, 1258-59 (10th Cir. 1998) (focusing on the logic prong); *United States v. Simone*, 14 F.3d 833, 838-39 (3d Cir. 1994) (same).

Amendment right of access to them.[26]

The Fourth Circuit has held that there is no First Amendment right to search warrant affidavits, although there is a common law right to them, because of the long history of sealing such proceedings. *Baltimore Sun Co. v. Goetz*, 886 F.2d 60, 64-65 (4th Cir. 1989). That decision does not mean that there is no First Amendment right to § 2703 orders and applications. The principal concern on which the Fourth Circuit relied in holding that there was no First Amendment right of access to an affidavit—avoiding tipping off the subject of the search until after the warrant was executed "lest he destroy or remove evidence," *id.* at 64 (citation omitted)—is not present here because the government decided to unseal the Twitter Order. Nor is it ever applicable to § 2703 orders; such orders are issued to third parties for records under their control, so there is little fear that tipping off the subject of the search will lead to the destruction of evidence. In addition, unlike search warrant proceedings, § 2703 proceedings have no centuries-long, established tradition of closure. Indeed, in some circumstances, § 2703 orders are not secret at all. Finally, court orders, unlike search warrant affidavits, are core judicial records, subject to the right of access.

2. The Government Cannot Meet Its Heavy Burden To Overcome The Presumption Of Access To The Sealed Documents.

In addition to applying the wrong legal tests, the Magistrate erred by not considering the Parties' and the public's significant interests in access, and whether the government's interests were compelling and the sealing narrowly tailored. Instead, the Court decided that because, in its view, there was a countervailing reason to keep the documents sealed, they should stay sealed. That was improper. Had these issues been considered, it would have been apparent that the government has not met its heavy burden.

---

[26] Where, as here, the First Amendment right of access attaches, it "may be overcome only by an overriding interest based on findings that closure is essential to preserve higher values and is narrowly tailored to serve that interest." *Press-Enterprise*, 464 U.S. at 510; *see Va. Dep't of State Police*, 386 F.3d at 575 (requiring a compelling interest).

a. The Unsealing Of The Twitter Order Removes The Justification For Continued Sealing Of The Sealed Documents.

Because the government chose to unseal the Twitter Order, the existence of the underlying criminal investigation is now known, as is the fact that it seeks information about the Parties. The traditional justifications for secrecy of investigations—to avoid tipping off potential subjects that they are being investigated and to avoid destruction of evidence—are therefore absent here. *See, e.g.*, *Va. Dep't of State Police*, 386 F.3d at 575 (holding that the government does not have a compelling interest in keeping information secret if it is already publicly known); *In re The Herald Co.*, 734 F.2d 93, 101 (2d Cir. 1984) (closure impermissible where information "sought to be kept confidential has already been given sufficient public exposure").

The Magistrate's reliance on *Moussaoui*, Op. at 18, is misplaced. *Moussaoui* does not "reject" the argument that sealing is not necessary for all matters already in the public record; it merely rejects the principle if the source of the public information is the media. 65 F. App'x at 887 n.5. Where, as here, the source of the information is the government itself, continued sealing is not appropriate. *Id.* ("[I]t is one thing for a reporter or author to speculate or guess that a thing may be so or even, quoting undisclosed sources, to say that it is so; it is quite another thing for one in a position to know of it officially to say that it is so.") (citation omitted).

The only potential interest that conceivably remains post-unsealing of the Twitter Order is that unsealing might reveal the names of "targets and witnesses" to the government's criminal investigation. Op. at 18. Notably, however, the Magistrate does not state that the identities of other individuals would be revealed if the remaining documents were unsealed. Instead, what unsealing would likely reveal are efforts to get other information about these same individuals.

Nor can continued sealing be justified on the grounds that it protects the names of the other companies who received § 2703 orders. Those companies are large entities over whom the Parties have little, if any, influence, and it is farfetched to believe that the Parties could intimidate those companies into destroying evidence. Moreover, the Parties already know the

identity of the other online service providers that they use, so unsealing documents disclosing those names would not lead to any additional risk of the destruction of evidence. In any event, to the extent unsealing would disclose anyone not yet publicly identified, and the Court concludes that doing so would cause serious harm to the investigation, the required solution, as described below, would be to unseal the documents with those names redacted.

At a minimum, given that disclosing the Twitter Order was "in the best interest of the investigation," Ex. 3, the government should be required to come forward with compelling reasons why continued sealing of any other § 2703 orders, as well as the other Twitter-related documents, is justified, and why those reasons heavily outweigh the interests of the Parties and the public in access.

b. The Magistrate Failed To Consider The Parties' Significant Interests In Unsealing The Documents.

Before the Magistrate, the Parties explained in detail why they needed the documents unsealed. *See* Dkt. No. 3 at 10-14. The Magistrate erred in largely ignoring these interests.

The Parties have a substantial interest in learning about the government's efforts to obtain their communications records so that they can take steps to protect their constitutional and statutory rights. The December 14 Order requires Twitter to produce records related to the Parties' communications on Twitter, regardless of any connection to WikiLeaks. Had that Order not been disclosed, the Parties would have been unable to mount a challenge to prevent the violation of their rights. Similarly, absent unsealing of any other § 2703 orders to other companies, the Parties will not be able to challenge them. They will also be hindered in challenging the Twitter Order or the other orders if they are prevented from learning the legal arguments and non-confidential facts that the government has articulated as a basis for obtaining the requested information.

The government's demands implicate the Parties' constitutional rights. Like many people, the Parties use multiple Internet communications services for self-expression,

publication, and association. As discussed earlier, the information demanded concerning their Twitter communications will reveal personal, intimate matters about their lives, expressive activities, and associations, regardless of any relationship between those communications and WikiLeaks. *See supra* at 2, 3-4. Combining this information with the Parties' records from their other private communications accounts will provide an even deeper and more invasive glimpse into their daily thoughts, associations, and activities. Based on the existence of the Twitter Order, the Parties reasonably believe that the government has sought information about their communications from other providers, and that these § 2703 orders and related documents remain under seal.[27]

Where, as here, a subpoena or *ex parte* court order to a third party implicates an individual's First Amendment rights, that individual has the right to challenge the request. *See, e.g.*, *Eastland*, 421 U.S. at 501 & n.14; *see also id.* at 514 (Marshall, J., concurring) (subject must be given a forum to "assert its constitutional objections to the subpoena, since a neutral third party could not be expected to resist the subpoena by placing itself in contempt").[28] Because continued sealing of the § 2703 orders and applications would frustrate the Parties' ability to exercise their right to challenge the § 2703 orders, they have significant interests in unsealing them. The Magistrate erred in failing to consider these interests.

---

[27] Neutral observers share the Parties' belief. *See, e.g.*, Gellman, *Twitter, Wikileaks, and the Broken Market for Consumer Privacy*, *supra*; Glenn Greenwald, *DOJ Subpoenas Twitter Records of Several WikiLeaks Volunteers*, Salon.com, Jan. 7, 2011, *available at* http://www.salon.com/news/opinion/glenn_greenwald/2011/01/07/twitter.

[28] *See also, e.g.*, *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); *In re First Nat'l Bank*, 701 F.2d at 117-19; *Local 1814, Int'l Longshoremen's Ass'n, AFL-CIO v. Waterfront Comm'n of N.Y. Harbor*, 667 F.2d 267, 271, 274 (2d Cir. 1981).

c. The Magistrate Ignored The Public's Significant Interest In Obtaining Access To The Sealed Documents.

The public also has an immense interest in unsealing.[29] The Magistrate relegated these interests to one sentence, Op. at 18, and failed to weigh them against the government's interests.

The sealed documents concern a matter of national importance—the ongoing debate about WikiLeaks' publications. Dkt. No. 3 at 22-24. The investigation of WikiLeaks has sparked a robust public debate involving issues of national security, government secrecy, and the First Amendment. That debate has included Congressional hearings, proposed legislation, reconsideration of information security procedures, and even commentary by the President.[30] Unsealing the sealed documents would contribute greatly to the public's ability to participate meaningfully in and evaluate this ongoing debate.

In addition to the significant public interest in this investigation, the public also has a substantial interest in knowing about the government's electronic surveillance of lawful Internet activities. An increasing percentage of personal and business activities are conducted online each year.[31] Recent developments in Internet technology, along with the advent of powerful portable computers, smart phones, cellular-based Internet, and ubiquitous wi-fi connections, have resulted in an ever-increasing amount of personal data being stored online and, thereby, potentially available to law enforcement.[32]

---

[29] The Parties have standing to assert the public's right of access to the sealed documents. *Leucadia, Inc. v. Applied Extrusion Techs., Inc.*, 998 F.2d 157, 167-68 (3d Cir. 1993).

[30] *See, e.g., The Espionage Act and the Legal and Constitutional Issues Raised by WikiLeaks: Hearing Before the H. Comm. On the Judiciary*, 111th Cong. (Dec. 16, 2010); *Securing Human Intelligence and Enforcing Lawful Dissemination Act*, H.R. 6506, 111th Cong. (2010); OMB Watch, *In WikiLeaks' Wake, Administration Tightens Information Security*, Jan. 11, 2011, *available at* http://www.ombwatch.org/node/11452; *Obama Calls WikiLeaks' "Deplorable,"* Reuters, Dec. 11, 2010, *available at* http://www.reuters.com/article/idUSTRE6BA24B20101211.

[31] *See* Pew Internet & American Life Project, Online Activities, 2000-2009, *available at* http://pewinternet.org/Static-Pages/Trend-Data/Online-Activities-20002009.aspx.

[32] *See generally* Paul Lanois, *Caught in the Clouds: The Web 2.0, Cloud Computing, and*

Because of this, Congress is now considering how to update the Electronic Communications Privacy Act, of which the law at issue here, the SCA, constitutes Title II.[33] Because the Twitter Order has been unsealed and the Parties now have an opportunity to challenge it, this case presents a rare and valuable opportunity for the public and Congress to learn about electronic surveillance orders and the nature and scope of the government's use of them as part of evaluating how the SCA may need to be updated in the digital age. Thus, even if this were not a case where these particular documents are of public concern, there would still be a significant public benefit in unsealing them. *See United States v. U.S. Dist. Court (Keith),* 407 U.S. 297, 317 (1972) ("[T]hose charged with [the] investigative and prosecutorial duty should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks.").

Finally, openness is particularly critical here because the public has a "magnified" interest in judicial records relating to law enforcement and the criminal justice system. *In re Application*, 923 F.2d at 330-31; *see also Press-Enterprise*, 464 U.S. at 508 (discussing how "openness" enhances "fairness"). The Magistrate erred in not weighing these interests in determining whether to keep the materials sealed.

3. The Generic Interests In Secrecy Proffered By The Government Are Not Sufficient To Satisfy Its Heavy Burden.

In contrast to these significant, specific interests in favor of access, the government's only argument is that this is a pre-indictment, ongoing investigation and that secrecy is therefore necessary. The government makes this assertion without explaining why, in these circumstances and as to these documents, sealing is necessary. That is not sufficient to satisfy the government's

---

Privacy?, 9 Nw. J. Tech. & Intell. Prop. 29 (2010).

[33] *See, e.g.*, *The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary*, 111th Cong. (Sept. 22, 2010); *ECPA Reform and the Revolution in Cloud Computing: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the*

heavy burden, and it is at odds with the Fourth Circuit cases establishing that sealing is not warranted simply because there is an ongoing investigation or no indictment yet.

Because "not every release of information contained in an ongoing criminal investigation file will necessarily affect the integrity of the investigation," generalized interests in "protecting the integrity of an ongoing law enforcement investigation" cannot justify sealing judicial documents. *Va. Dep't of State Police*, 386 F.3d at 579. Thus, "it is not enough simply to assert this general principle without providing specific underlying reasons for the district court to understand how the integrity of the investigation reasonably could be affected by the release of such information" with respect to each document that the government wishes to keep secret. *Id.* Instead, it is the government's burden to present "specific facts and circumstances" to justify "the effort to restrict public access" to each specific document. *Id.*; *see Baltimore Sun*, 886 F.2d at 64-66; *In re Wash. Post Co.*, 807 F.2d 383, 391-92 (4th Cir. 1986).

The government has not come close to meeting this burden. The Magistrate cited the following general "reasons" for why documents related to ongoing investigations should be sealed: (1) "[s]ecrecy protects the safety of law enforcement officers;" (2) it "prevents destruction of evidence;" (3) it "protects witnesses from intimidation or retaliation;" and (4) it "prevents unnecessary exposure of those who may be the subject of an investigation, but are later exonerated." Op. at 17. None of these traditional rationales for secrecy are present here. As noted above, the targets, subjects, and witnesses of this investigation already know who they are due to the government's decision to unseal the Twitter Order. Any risk of destruction of evidence has already passed, as has the risk of witness intimidation or retaliation, were that even a possibility here. Nor is there any risk to law enforcement officer safety from unsealing—in fact, the government did not even claim such an interest. Finally, sealing is not necessary here to prevent the unnecessary exposure of potentially innocent parties—the Parties have already been

---

Judiciary, 111th Cong. (Sept. 23, 2010).

exposed by the government itself.

Stripped of these traditional reasons for secrecy, the only remaining argument is essentially that all pre-indictment judicial records should *per se* be sealed, without regard for the circumstances involved. Op. at 18. That is not so. There is a presumption of access to "all judicial records and documents." *Va. Dep't of State Police*, 386 F.3d at 575 (emphasis added); *see also Nixon,* 435 U.S. at 602. In fact, in *Baltimore Sun*, the Fourth Circuit rejected this argument, holding that there is a right of access to pre-indictment search warrant affidavits, and vacating the district court's sealing of them which was based merely on a general finding that "the public interest in the investigation of crime outweighed the [media's] interest in access prior to return of the indictments." 886 F.2d at 66; *see also Va. Dept. of State Police*, 386 F.3d at 579-80 (affirming district court's unsealing of documents related to an ongoing investigation).[34]

4. The Magistrate Erred By Not Expressly Ruling On Whether Each Specific Document At Issue, Including The § 2703 Orders To Other Companies, Should Be Sealed.

The Fourth Circuit has made clear that courts are required to make a specific determination as to *each* document sought to be sealed that the asserted interest in secrecy heavily outweighs the public's right of access to it. *Stone*, 855 F.2d at 181 (courts must weigh competing interests "with respect to each document sealed"). The Magistrate failed to do so, instead denying the Parties' motion to unseal as to all of the "10-gj-3793 documents." Op. at 19.

One category of documents deserves special consideration: the § 2703 orders to other companies. Given that it was "in the best interest of the investigation" to unseal the Twitter Order, Ex. 3, there is no reason why these other orders cannot also be unsealed. The Magistrate erred in not requiring the government to provide a specific rationale for why any similar orders to other companies should remain unsealed.

[34] The Magistrate incorrectly asserted that the Parties "present no authority for the proposition that the public has a right of access to documents related to an ongoing investigation." Op. at 18. In fact, the Parties cited two Fourth Circuit cases for this proposition. *Va. Dept. of State Police*,

Additionally, the Magistrate's failure to proceed document-by-document has led to the untenable result that even though the government has agreed that its motion to unseal the Twitter Order should be unsealed, *see* Dkt. No. 34, at 4, that document, which is on the 10-gj-3793 docket, still remains sealed under the Magistrate's Order, and the Parties (and the public) have not seen it.

The absence of a document-by-document analysis is especially problematic given that there is not a public docket reflecting the documents that are under seal. Because the absence of public docketing violates clear Fourth Circuit caselaw, the Parties asked the Magistrate to issue an order requiring public docketing sufficient to provide the public with notice of any motions or orders sealing documents related to this case. The Magistrate has not yet ruled on this request, accentuating the need for a document-by-document analysis.

5. The Magistrate Failed To Consider Alternatives To Sealing.

The Magistrate also erred by failing to consider alternatives to complete sealing. Because the right to access is such a fundamental right, courts must first "consider less drastic alternatives to sealing," and must not seal documents completely if it is possible to accommodate the government's interests by redacting specific information, even in pre-indictment proceedings. *Stone*, 855 F.2d at 181; *see also Baltimore Sun*, 886 F.2d at 66 (holding that the judicial officer "must consider alternatives to sealing the documents," which "ordinarily involves disclosing some of the documents or giving access to a redacted version"); *Moussaoui*, 65 F. App'x at 889 ("[S]ealing an entire document is inappropriate when selective redaction will adequately protect the interests involved"). If a court decides complete sealing is necessary, it is required to state "the reasons for rejecting alternatives." *Stone*, 855 F.2d at 181 (quotation omitted).

Thus, even if the government here had shown that the release of certain information in the sealed documents would cause significant harm to its investigation, the appropriate response

---

386 F.3d at 579-80; *Baltimore Sun*, 886 F.2d at 66.

would have been for that specific, harmful information to be redacted prior to unsealing. For example, if the sealed documents contain the names of targets or witnesses not already revealed by the unsealing of the Twitter Order and revealing those names would seriously jeopardize the investigation, the correct procedure would have been for the Magistrate to unseal the documents, and to order those names redacted. The Magistrate failed to do so. Nor did the Magistrate explain why such redactions were not possible. That was in direct violation of long-established Fourth Circuit case law. *See. e.g., Baltimore Sun*, 886 F.2d at 65-66; *Stone*, 855 F.2d at 181; *In re Knight Publ'g Co.*, 743 F.2d 231, 235 (4th Cir. 1984).

IV. CONCLUSION

In light of the issues highlighted above, the Parties request that the Court vacate the Magistrate's March 11 Order and issue a new order (1) vacating the Twitter Order as violative of § 2703, the First Amendment, and the Fourth Amendment and (2) granting the Parties' Motion to Unseal with respect to all remaining, sealed documents relating to the Twitter Order and any similar § 2703 orders to entities other than Twitter.

Dated: March 25, 2011

By: /s/ John W. Keker

John W. Keker (admitted *pro hac vice*)
Rachael E. Meny (admitted *pro hac vice*)
Steven P. Ragland (admitted *pro hac vice*)
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

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

Attorneys for JACOB APPELBAUM

Dated: March 25, 2011

By: /s/ John D. Cline

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

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

Nina J. Ginsberg, VSB No. 19472
DIMUROGINSBERG, P.C.
908 King Street, Suite 200
Alexandria, VA 22314
Telephone: 703.684.4333
Facsimile: 703.548.3181
Email: nginsberg@dimuro.com

Attorneys for ROP GONGGRIJP

Dated: March 25, 2011

By: /s/ Cindy A. Cohn

Cindy A. Cohn (admitted *pro hac vice*)
Lee Tien (admitted *pro hac vice*)
Kevin S. Bankston (admitted *pro hac vice*)
Marcia Hofmann (admitted *pro hac vice*)
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 (admitted *pro hac vice*)
Benjamin Siracusa-Hillman (admitted *pro hac vice*)
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

Rebecca K. Glenberg, VSB No. 44099
AMERICAN CIVIL LIBERTIES UNION OF VIRGINIA FOUNDATION, INC.
530 E. Main Street, Suite 310
Richmond, VA 23219
Telephone: 804.644.8080
Facsimile: 804.649.2733
Email: rglenberg@acluva.org

Jonathan Shapiro
GREENSPUN, SHAPIRO, DAVIS & LEARY, P.C.
3955 Chain Bridge Road
Second Floor
Fairfax, VA 22030
Telephone: 703.352.0100
Facsimile: 703.591.7268
Email: js@greenspunlaw.com

Attorneys for BIRGITTA JONSDOTTIR

CERTIFICATE OF SERVICE

I hereby certify that on this 25th day of March, 2011, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to the following counsel of record:

Tracy D. McCormick
U.S. Attorney's Office
2100 Jamieson Avenue
Alexandria, VA 22314
Telephone: 703-299-3175
Email: tracy.mccormick@usdoj.gov

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

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

Jonathan Shapiro
GREENSPUN, SHAPIRO, DAVIS
& LEARY, P.C.
3955 Chain Bridge Road
Second Floor
Fairfax, VA 22030
Telephone: (703) 352-0100
Facsimile: (703) 591-7268
Email: js@greenspunlaw.com

John K. Roche
Perkins Coie, LLP
700 13th Street, N.W., Suite 600
Washington, DC 20005
Telephone: 202-654-6200
Facsimile: 202-654-6211
Email: jroche@perkinscoie.com

/s/_____

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