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