

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF VIRGINIA  
Alexandria Division

IN RE APPLICATION OF THE	)	
UNITED STATES OF AMERICA	)	MISC. NO. 10GJ3793
FOR AN ORDER PURSUANT TO	)	No. 1:11DM3
18 U.S.C. § 2703(d)	)	

**GOVERNMENT’S RESPONSE TO OBJECTIONS OF THREE TWITTER  
SUBSCRIBERS TO MAGISTRATE JUDGE’S MARCH 11, 2011, OPINION  
DENYING MOTION TO VACATE AND DENYING IN PART MOTION TO UNSEAL**

The United States of America, by Neil H. MacBride, United States Attorney for the Eastern District of Virginia, responds as follows to the Objections of Jacob Appelbaum, Birgitta Jonsdottir, and Rop Gonggrijp (the “Subscribers”) to Magistrate Judge Buchanan’s Memorandum Opinion and Order of March 11, 2011 (the “Opinion”), denying their Motion to Vacate and denying in part their Motion to Unseal:

**I. *Background***

On December 14, 2010, Magistrate Judge Buchanan entered a sealed order (the “Twitter Order” or “Order”) pursuant to 18 U.S.C. § 2703(d) directing Twitter, Inc., to disclose certain non-content records and other information pertaining to four Twitter accounts, including those identified as rop\_g; ioerror; and birgittaj. For each account, the Order identified specific customer or subscriber information for the period November 1, 2009, to the date of the Order, as well as IP addresses and other records of user activity for connections made to the Twitter accounts. *See* (Order, Attachment A.)

On January 5, 2011, the magistrate judge unsealed the Order and authorized Twitter to disclose it. Twitter thereafter gave notice of the Order to the three Subscribers: Jacob Appelbaum (associated with ioerror), Birgitta Jonsdottir (associated with birgittaj), and Rop Gonggrijp (associated with rop\_g).

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. *See* (Gov't Obj. to Mot. of Three Twitter Subscribers to Vacate Order at 2 n.1.) On January 26, 2011, the Subscribers moved to vacate the Order, citing a variety of statutory and constitutional grounds, and also moved to unseal certain court records in this matter.<sup>1</sup> The government objected to both motions. On February 15, 2011, the magistrate judge heard oral argument on the Subscribers' motions.

On March 11, 2011, the magistrate judge issued the Opinion, which denied the Subscribers' motion to vacate, and denied in part, granted in part, and took under further consideration in part their motion to unseal. On March 25, 2011, the Subscribers filed objections to the Opinion. The government now responds to those objections

## **II. *Standard of Review***

The Subscribers ostensibly file their objections pursuant to Federal Rule of Criminal Procedure 59 or Federal Rule of Civil Procedure 72. (Subscribers' Obj. at 5.) Since this matter arises from the Subscribers' motion to vacate a § 2703(d) order that was issued in a pending grand jury investigation, the rules of criminal procedure apply. *See* Fed. R. Crim. P. 1; *United States v. Awadallah*, 349 F.3d 42, 49-55 (2<sup>nd</sup> Cir. 2003) (finding that "grand jury proceeding" is a "criminal proceeding" for purposes of the material witness warrant statute). *Cf. Application of*

---

<sup>1</sup>The Subscribers challenged the Order with respect to the three Twitter accounts with which they are identified. But with respect to the fourth Twitter account, WikiLeaks, no party raised objections as to Twitter's production of records related to it. No person appeared on behalf of Wikileaks in the proceedings before the magistrate judge, who dismissed as moot Twitter's motion for clarification related to production of records from the WikiLeaks account. Twitter did not object to the dismissal. Thus, both the owner of the Wikileaks Twitter account and Twitter itself have waived any right to appeal the Order's directive to produce records relating to the account. *See Wells v. Shriners Hospital*, 109 F.3d 198, 199 (4<sup>th</sup> Cir. 1997) ("the consequence of failing to file objections is waiver of the right to appeal").

*the United States for an Order Authorizing the Interception of Oral Communications*, 563 F.2d 637, 641 (4<sup>th</sup> Cir. 1977) (denial of order for wiretap interception was not criminal proceeding because it arose prior to indictment and grand jury proceeding). Accordingly, this Court should review the Subscribers' objections under Rule 59.<sup>2</sup>

Rule 59(a) authorizes a party to file objections to a magistrate judge's order that determines "any matter that does not dispose of a charge or defense." In contrast, Rule 59(b) permits 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."

Here, the magistrate judge's denial of the Subscriber's motion plainly "does not dispose of any charge or defense," Fed. R. Crim. P. 59(a), but instead orders the disclosure of records by a third party in the course of an ongoing grand jury investigation. It is therefore a non-dispositive order, and the Subscriber's objections to it are governed by Rule 59(a).<sup>3</sup> Under that Rule this Court must determine whether the magistrate judge's ruling was "contrary to law or

---

<sup>2</sup> Rule 59's procedures for objections 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) of that Rule. Although no individual referral was made in this case, the 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. Crim. R. 5.

<sup>3</sup>At least two district courts have applied Rule 59(a) in reviewing magistrate judge decisions about § 2703(d) orders. *See In re U.S. for Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 2008 WL 4191511, at \*1 (W.D. Pa. 2008) (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)), *vacated on other grounds*, 620 F.3d 304 (3d Cir. 2010); *In re U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Information*, 2006 WL 2871743, at \*1 (E.D. Wis. 2006) (same).

clearly erroneous,” and should not modify or set aside the ruling 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 3245896, 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”); *Tafas v. Dudas*, 530 F. Supp. 2d 786, 792 (E.D. Va. 2008) (in civil case, “[a]s a non-dispositive matter, the review of a magistrate’s discovery order is properly governed by the ‘clearly erroneous or contrary to law’ standard of review”). Further, a finding is “clearly erroneous” when, although there is evidence to support it, the reviewing court on the entire evidence is left with the definite and firm conviction that a mistake has been committed. *Tafas*, 530 F. Supp. 2d at 792.

The Subscribers assert that the Opinion is “dispositive” as to their claims, thereby requiring this Court to review their objections under Rule 59(b)’s *de novo* standard. (Subscribers’ Obj. at 5.) But Rule 59(b) is inapplicable here. Pursuant to Local Criminal Rule 5 and 18 U.S.C. § 2703(d), the magistrate judge issued an order, not “proposed findings and recommendations” subject to review under Rule 59(b). Furthermore, the Subscribers’ original motions were not “dispositive” under the Rule’s plain language, because they did not constitute motions to dismiss or quash charges or suppress evidence, and their resolution did not otherwise “dispose of a charge or offense.” Fed. R. Crim. P. 59(b)(1).

In support of their claim for *de novo* review, the Subscribers rely exclusively on *ALCOA v. U.S. Envtl. Prot. Agency*, 663 F.2d 499, 501-02 (4th Cir. 1981). (Subscribers’ Obj. at 5.) There the Fourth Circuit held that a motion to quash an administrative search warrant was dispositive for purposes of 28 U.S.C. § 636(b) because it “was not a ‘pretrial matter’ but set forth

all of the relief requested.” *ALCOA* is distinguishable, however, since it involved an administrative investigation and proceeding, not a grand jury investigation. Thus, in *ALCOA* the magistrate’s decision on a motion to quash the administrative warrant was dispositive because it resolved the sole proceeding before the court. In this case, however, Magistrate Judge Buchanan’s decision was not dispositive because it did not resolve the entire case; an ongoing grand jury proceeding remains. See *In re Oral Testimony of a Witness Subpoenaed*, 182 F.R.D. 196, 200-202 (E.D. Va. 1998). Therefore, the standard for this Court’s review of the Subscribers’ objections is whether Judge Buchanan’s ruling was “contrary to law or clearly erroneous.” Fed. R. Crim. P. 59(a).

Finally, with respect to the Subscribers’ objections to the denial of their motion to unseal court records, because Magistrate Judge Buchanan was the judicial officer who issued the § 2703(d) order, her “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 *Nixon v. Warner Communications, Inc.*, 435 U.S. 589, 599 (1978) (noting judicial agreement “that the decision as to access is one best left to the sound discretion of the trial court”); *Media General Operations, Inc. v. Buchanan*, 417 F.3d 424, 429 (4th Cir. 2005) (quoting *Goetz*); *Tafas*, 530 F. Supp. 2d at 792.

### **III. Argument**

#### **A. The Magistrate Judge Correctly Ruled That the Subscribers Have Not Established Standing To Move to Vacate the Twitter Order.**

The magistrate judge correctly concluded that the Subscribers have not established standing to move to vacate the Twitter Order. (Op. at 4.) The Stored Communications Act (18

U.S.C. §§ 2701-2712) (“the SCA”) precludes the Subscribers from moving to vacate the Twitter Order for a putative nonconstitutional violation of § 2703(d). 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; *cf. United States v. Clenney*, 631 F.3d 658, 667 (4th Cir. 2011) (“Congress made it clear that it did not intend to suppress evidence gathered as a result of § 2703(c) violations”). The Subscribers have identified no authority, in the SCA or elsewhere, that allows them to challenge the Twitter Order on nonconstitutional grounds.

Section 2704(b) is the SCA’s sole provision that may give a customer or subscriber authority to challenge on nonconstitutional grounds an order issued under § 2703(d). However, the magistrate judge correctly concluded that the Subscribers cannot avail themselves of that provision because the Order requires disclosure only of “non-content” information, and “targets of court orders for non-content or records information may not bring a challenge under 18 U.S.C. § 2704.”<sup>4</sup> (Op. at 4 (citing § 2704(b)(1)(A)).) Although the Subscribers suggest in passing that IP address information “may not properly constitute a mere records disclosure,”<sup>5</sup> (Subscribers’

---

<sup>4</sup>The government disagrees with the Subscribers’ contention that “[t]here is no basis in the statute to distinguish between standing to challenge orders that seek content and orders that do not.” (Subscribers’ Obj. at 6-7.) Section 2704(b)(1)(A) plainly provides that a customer or subscriber may bring a § 2704(b) challenge only when the government has sought the contents of his electronic communications. *See* 18 U.S.C. § 2704(b)(1)(A). Moreover, the government must provide notice under § 2703(b)(1) when it obtains the contents of a customer or subscriber’s communications with a subpoena or court order, but not when it obtains “non-content” information under § 2703(c).

<sup>5</sup> Notwithstanding the Subscribers’ contrary suggestion, 18 U.S.C. § 2703(c) expressly contemplates “the disclosure of IP addresses recorded over a period of time” and treats it as a “records disclosure.” (Subscribers’ Obj. at 7 n.14.) 18 U.S.C. § 2703(c)(2)(E) specifically authorizes use of a subpoena to obtain a customer or subscriber’s “telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address.” *Id.* Moreover, 18 U.S.C. § 2703(c)(1) authorizes issuance of a § 2703(d) court order

Obj. at 7 n.14), they acknowledge that they cannot move to vacate the Order under § 2704(b), and even suggest additional reasons why a § 2704(b) challenge may not be available to them. In short, the magistrate judge correctly determined that the SCA provides no judicial remedies that would allow the Subscribers to move to vacate the Twitter Order for an alleged nonconstitutional violation. The magistrate judge also properly ruled that the Subscribers have no basis to bring “a viable constitutional challenge” to the Order, (Op. at 5), because, as shown *infra*, the disclosures authorized by the Order do not infringe the Subscribers’ First or Fourth Amendment rights

The Subscribers respond that they should be allowed to move to vacate the Twitter Order “for both its statutory and constitutional transgressions” because, among other things, “[f]undamental fairness and due process demand that the Parties have the right to challenge disclosure of their records here.” (Subscribers’ Obj. at 7.) Yet the Subscribers cite no case holding that fundamental fairness or due process requires that they be permitted to impede valid legal process issued to third parties in an ongoing criminal investigation. Instead, the Subscribers cited several civil cases that the magistrate judge rightly concluded were not on point.<sup>6</sup> (Op. at 5; Subscribers’ Reply Br. at 2-3; Subscribers’ Obj. at 6-7.)

**B. The Magistrate Judge Properly Held That the Twitter Order Complied with the SCA.**

The magistrate judge correctly ruled that the Order was properly issued under the SCA. (Op. at 7.) Under 18 U.S.C. § 2703(d), a court may issue an order for disclosure under 18 U.S.C.

---

to obtain “a record or other information pertaining to a subscriber . . . or customer . . . (not including the contents of communications).” *Id.* Because an IP address does not include the contents of any communications, its disclosure may be compelled under 18 U.S.C. § 2703(c)(1).

<sup>6</sup>The Subscribers also purport to object to the magistrate judge’s ruling that, “even when a subscriber is not entitled to notice under the SCA, she lacks standing to challenge an order of which she becomes aware.” (Subscribers’ Obj. at 7.) However, the magistrate judge’s standing analysis did not discuss notice at all. *See* (Op. at 4-5.)

§§ 2703(b) or (c) if the government provides “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 magistrate judge concluded that the government met this standard when she issued the Order, and “remain[ed] convinced that the application stated ‘specific and articulable’ facts sufficient to issue the Twitter Order under § 2703(d).” (Op. at 7.) In so ruling, the magistrate judge noted that “the scope of the Twitter Order is appropriate even if it compels disclosure of some unhelpful information,” as “§ 2703(d) is routinely used to compel disclosure of records, only some of which are later determined to be essential to the government’s case.” (Op. at 7.)

The Subscribers maintain that the Magistrate improperly issued the Order because the government’s application (which the Subscribers have not seen) cannot possibly satisfy the “specific and articulable facts” standard. Their argument is meritless. “[T]he ‘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)). In other words, “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*, 631 F.3d 266, 291 (6th Cir. 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 rationale 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 (Subscribers’ Obj. at 8), 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. (Subscribers’ Obj. at 9.) The Subscribers’ argument is based on cases that discuss “materiality” in contexts very different from § 2703(d). *See* (Subscribers’ Obj. at 9); *United States v. Valenzuela-Bernal*, 458 U.S. 858, 867-73 (1982) (evaluating whether deportation of potential witnesses violated defendant’s constitutional rights); *Rovario 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 magistrate judge found that the application satisfied § 2703(d)’s requirements, including its stricture that the records sought be “material to an ongoing criminal investigation.” 18 U.S.C. § 2703(d).

Further, there is no merit to the Subscribers’ pronouncement that the records described in the Order cannot be “relevant and material to an ongoing criminal investigation” simply because, in the Subscribers’ view, much of their Twitter activity “has nothing to do with Wikileaks.”

(Subscribers’ Obj. at 8.)<sup>7</sup> By the Subscribers’ logic, the government could never use a § 2703(d)

---

<sup>7</sup>In any event, the government has already minimized to the extent possible inclusion of non-WikiLeaks-related information by agreeing to narrow Twitter’s response to non-content information concerning direct (i.e., private) messages only between the four identified accounts, *see supra* n.1, and to exclude records of user activity for connections to or from the accounts relating to public followers, Apache logs, or replies to Twitter feeds.

order to obtain email transaction logs or phone bills unless it could show that every email or phone call related directly to the crime under investigation. Indeed, such a standard could almost never be met. The government is aware of no court that has adopted such a restrictive view of § 2703(d). Nor is such a view required by law. *See* (Op. at 7 (“At an early stage, the requirement of a higher probable cause standard for non-content information voluntarily released to a third party would needlessly hamper an investigation.”)); *In re Subpoena Duces Tecum*, 228 F.3d 341, 348-49 (4<sup>th</sup> Cir. 2000) (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”).

**C. The Magistrate Judge Correctly Rejected the Subscribers’ Constitutional-Avoidance Argument.**

Citing the *Third Circuit Opinion*, 620 F.3d 304, 313 (3d Cir. 2010), the Subscribers contend that the language of 18 U.S.C. § 2703(d) grants courts discretion to deny – and, by extension, vacate – orders under that section, even when the government has made the requisite factual showing. *See* (Subscribers’ Obj. at 9.) The Subscribers further argue that, because they have raised “serious” constitutional questions, the Court should vacate the Order. *See id.* But the magistrate judge “decline[d] to deviate from the standard expressly provided in § 2703(d),” noting that “[a]t an early stage, the requirement of a higher probable cause standard for non-content information voluntarily released to a third party would needlessly hamper an investigation.” (Op. at 7.)

The magistrate judge was manifestly correct. First, the plain language of § 2703(d) contradicts the alternative reading urged by the Subscribers. That statute provides, “A court order for disclosure . . . *may be issued* by any . . . court of competent jurisdiction *and shall issue*

*only if* the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the . . . records or other information sought, are relevant and material to an ongoing criminal investigation” (emphasis supplied). The Subscribers’ argument relies on a Third Circuit case interpreting the phrase “may be” to imply court discretion and finding that this reading was bolstered by § 2703(d)’s “only if” phrase. As a result, the Third Circuit found that the “specific and articulable facts” requirement was a necessary but not a sufficient condition for obtaining a 2703(d) order. *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” and that such a requirement was “an option to be used sparingly”). But as the government argued before the magistrate judge, the Third Circuit’s strained reading of § 2703(d) is not binding on this Court and should be rejected because it renders superfluous the phrase “and shall issue” in § 2703(d). The Third Circuit essentially interpreted § 2703(d) to mean that an order “may be issued by . . . a court of competent jurisdiction [ ] only if the governmental entity offers specific and articulable facts . . . .” Such an interpretation renders the phrase “and shall issue,” which should precede the phrase “only if,” devoid of meaning. This violates the cardinal principle of statutory construction that a statute ought to be construed so that no word or clause is rendered superfluous. *Gunnells v. Healthplan Servs.*, 348 F.3d 417, 439-40 (4th Cir. 2003). Giving meaning to all of the words in § 2703(d) results in the opposite conclusion: the statute requires a court to issue a 2703(d) order when the application satisfies the “specific and articulable facts” standard of § 2703(d) and otherwise complies with the law. Thus, § 2703(d) provides no basis for a court to exercise discretion to vacate a valid order that was issued upon a finding of “specific and articulable facts.”

Second, as the magistrate judge implicitly recognized, and as further explained *infra*, the Subscribers have utterly failed to raise “serious” constitutional questions that warrant avoidance. Under the doctrine of constitutional avoidance, “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, the Subscribers have raised no serious doubts as to § 2703(d)’s constitutionality, and so the Court need not explore alternative readings of the statute to avoid constitutional questions that do not exist.

**D. The Magistrate Judge’s Holding that the Order Does Not Abridge the Subscribers’ First Amendment Rights Is Not Contrary to Law.**

The Subscribers argue that the Order has a “chilling effect” on their speech and association rights under the First Amendment, and on the right of Twitter users in general, and that the government is required to show that the specific information sought under § 2703(d) bears a “substantial relation to an overriding and compelling state interest.” (Subscribers’ Obj. at 11-13.) In the Opinion the magistrate judge squarely rejected those claims, finding that the Subscribers, “who have already made their Twitter posts and associations publicly available,” had “fail[ed] to explain how the Twitter Order has a chilling effect.” (Op. at 9.) The magistrate judge also found that the government had a “legitimate interest in the disclosures sought,” that the Order is “reasonable in scope,” and that the Order “does not seek to control or direct the content of [the Subscribers’] speech or association. Rather, it is a routine compelled disclosure of non-content information which [the Subscribers] voluntarily provided to Twitter pursuant to Twitter’s Privacy Policy.” (Op. at 9-10.) The magistrate judge also observed that the First

Amendment's freedom of association "does not shield members [of organizations] from cooperating with legitimate government investigations." (Op. at 8.)

The Subscribers object that where an investigation allegedly intrudes into an area of protected First Amendment rights, the government must convincingly show a "substantial relation" between the information sought and a subject of overriding and compelling state interest, and that here the magistrate judge "failed to evaluate this intrusive demand with the requisite scrutiny." (Subscribers' Obj. at 11-12.) But their objection fails in several respects. First, its premise - that in directing production of non-content information about Twitter communications the Order "intrudes" into an area of protected First Amendment rights - is false. Indeed, as shown below, the implication of the Subscribers' claim -- that in a criminal investigation ordinary non-content communications records cannot constitutionally be sought absent proof of a "substantial relation" between the records and an "overriding and compelling" state interest -- is absurd.

As the magistrate judge found, the Order directs a "routine" disclosure by a third party in a criminal investigation. (Op. at 9.) The Order has no essential relation to First Amendment-protected activity other than that its object is a type of non-content records related to communications. Of course, a great variety of commonplace communications records may properly be gathered in an investigation - without resort to the "substantial relation" test, or any test other than relevance. For example, visitor logs identify visitors to jail cells and corporate offices, and calendars document meetings. Mail covers and shipping records track correspondence. Telephone tolls and pen registers reveal incoming and outgoing calls. Skype connection records show the use of on-line video conferencing facilities. And so on. To be sure, all of these kinds of records, like the sought-after information held by Twitter, potentially relate

to instances of protected speech, or may demonstrate “associations” among particular persons. But such records nonetheless are widely subpoenaed by grand juries without raising “chilling effects,” or occasioning constitutional litigation and delays. Likewise here: Twitter’s non-content and routinely collected subscriber and connection data are not specially insulated from investigative scrutiny merely because they relate to communications.

Second, assuming for argument’s sake that special scrutiny is required here, the “substantial relationship” test urged by the Subscribers is not the law. As the magistrate judge stated, the Fourth Circuit has not endorsed the “substantial relationship” test in the First Amendment context, and instead merely requires a district court faced with a constitutional challenge to prevent abuse and to “balance the possible constitutional infringement and the government’s need for documents . . . on a case-by-case basis and without putting any special burden on the government.” *In re Grand Jury 87-3 Subpoena Duces Tecum*, 955 F.2d 229, 234 (4<sup>th</sup> Cir. 1992); (Op. at 9). The magistrate judge concluded that the government had a legitimate interest in the records sought; that the Order was reasonable in scope (it extends only to four accounts over a seven-month period); and that there was “no indication of bad faith by the government.” (Op. at 10.) These factual findings were not clearly erroneous, Fed. R. Crim. P. 59(a), and under the applicable standard are sufficient to dispose of the Subscribers’ First Amendment claim.

Third, as the magistrate judge noted, even if the “substantial relationship” test did apply in this circuit and to the challenged Order, the Order would almost certainly pass constitutional muster, since “even courts that have adopted the test regularly refuse to quash subpoenas on First Amendment grounds.” (Op. at 9 n.3 (citing out-of-circuit cases).) In their objections the Subscribers cite no contrary authority. Indeed, it is difficult to imagine a more “overriding and

compelling” state interest than the prompt collection of relevant evidence in the investigation of serious crimes. And when that evidence relates to instances of communications already widely publicized and voluntarily conveyed to a third party the claim to abridgement of free speech or association rights is exceedingly weak. *Cf. Uphaus v. Wyman*, 360 U.S. 72, 81 (1959) (noting that state law required camp to maintain guest register, open to inspection, and that the state’s investigative interest was “sufficiently compelling to subordinate the interest in associational privacy of persons who, at least to the extent of the guest registration statute, made public at the inception the association they now wish to keep private”).

In summary, the Subscribers’ claim that Twitter’s non-content records are subject to heightened protections under the First Amendment is baseless. Moreover, under the case-by-case balancing test employed in this circuit, the magistrate judge was not clearly erroneous in finding that the government has a legitimate interest in the Twitter records, the Order’s scope is reasonable, and there is no bad faith. Finally, even if the “substantial relationship” test applied, the Order would not violate that test.

**E. The Magistrate Judge Correctly Rejected the Subscribers’ Fourth Amendment Challenge to the Twitter Order.**

The magistrate judge also correctly determined that the Order does not violate the Subscribers’ Fourth Amendment rights. The Subscribers identify only one aspect of the Order that supposedly implicates such rights: the Order’s directive that Twitter disclose “the IP addresses they used at particular dates and times when logging into their Twitter accounts.” (Subscribers’ Obj. at 13.) 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 “can be used to track the Parties’ locations in, and movements between, particular

private spaces over a period of time.” (Subscribers’ Obj. at 13.) However, as the magistrate judge held, the Subscribers have no Fourth Amendment interest in the IP address information, and are not entitled to relief on that ground.

IP addresses are analogous to telephone numbers. *See* (Op. at 13); *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*, 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. “When a user visits a website, the site administrator can view the IP address.” (Op. at 13 (citing *United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010).) Here, the magistrate judge specifically found that the Subscribers “voluntarily conveyed their IP addresses to the Twitter website, thus exposing the information to a third party administrator, and thereby relinquishing any reasonable expectation of privacy.” (Op. at 13.)

As the magistrate judge correctly noted, “the Fourth Amendment privacy expectation does not extend to information voluntarily conveyed to third parties.” (Op. at 11); *see Smith v. Maryland*, 442 U.S. 735 (1979) (holding that telephone users have no reasonable expectation of privacy in the telephone numbers they dialed because “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.”); *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”); *United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010) (recognizing



that subscriber had no reasonable expectation of privacy in certain information voluntarily conveyed to his phone and internet companies – *i.e.*, his name, email address, phone number, and physical address). Because the Subscribers voluntarily transmitted their IP addresses to Twitter to gain access to their Twitter accounts, they assumed the risk that Twitter would reveal the addresses to law enforcement agents and cannot now claim a reasonable expectation of privacy in Twitter’s records of their IP addresses. *See* (Op. at 13); *Forrester*, 512 F.3d at 510.

The Subscribers fail to cite any case holding that Internet users have a 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.<sup>7</sup> *See Christie*, 624 F.3d at 574 (“[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.”); *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.”). *See also Bynum*, 604 F.3d at 164. The magistrate judge correctly adopted the reasoning of these cases and held that the Subscribers lack a reasonable expectation of privacy in their IP address information. (Op. at 13.)

Further, there is no merit to the Subscribers’ contention that the magistrate judge should have departed from these cases and concluded that IP address records deserve Fourth Amendment protection because IP addresses “can be used to track the Parties’ locations in, and movements between, particular private spaces over a period of time.” (Subscribers’ Obj. at 13.)

---

<sup>7</sup>In addition, the Tenth Circuit found that “‘subscriber information’ provided to an internet provider is not protected by the Fourth Amendment’s privacy expectation.” *Perrine*, 518 F.3d at 1204.

As an initial matter, the Subscribers have identified “no authority finding that an IP address shows location with precision, let alone provides insight into a home’s interior or a user’s motion.” (Op. at 13.)

Moreover, business records do not become privileged merely because they contain information that might enable the government to discern a person’s location. For example, telephone users have no reasonable expectation of privacy in traditional land-line telephone records, even though 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. *See Smith*, 442 U.S. at 745 (concluding that phone user had no legitimate expectation of privacy in phone numbers he dialed, even when collected in real time). Further, the government is not required to obtain a warrant before compelling businesses to produce other types of 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 those records to discern the Subscribers’ locations at certain times.<sup>8</sup>

---

<sup>8</sup> The Subscribers attempt to buttress their location-based argument by citing *United States v. Karo*, 468 U.S. 705 (1984), and *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), but those tracking-device cases do not help their cause. *Karo* requires the government to obtain a warrant before using a tracking device to reveal information about the interior of a private location, *see* 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. *Maynard* also focuses on Fourth Amendment issues surrounding the use of tracking devices, rather than business records, and is inconsistent with Supreme Court precedent, including *Smith v. Maryland* and *Katz v. United States*, 389 U.S. 347 (1967), and in conflict with tracking-device decisions of other courts of appeals.

The Subscribers also argue that they did not voluntarily convey their IP addresses to Twitter when they logged into their Twitter accounts (Subscribers' Obj. at 14-15), because their IP addresses were "passively communicated without any action by, knowledge of, or visibility to, the user." (Op. at 13.) The magistrate judge correctly rejected this claim as "inaccurate." (Op. at 13.) The Subscribers did take actions to communicate their IP addresses to Twitter – they intentionally used Internet-connected devices to access their accounts and thereby sent their IP addresses to Twitter. Although the transmission of these IP addresses may not have been "visible" to the Subscribers, just as the transmission of a caller's own phone number to his phone company is not "visible" to the caller, the Subscribers nonetheless should have known that their Internet-connected devices were sending their IP addresses to Twitter so it could send the requested account information to those specific devices. Indeed, despite the Subscribers' contrary claims, the Subscribers' IP addresses are "analogous to dialing information" because Twitter needed this information to route the Subscribers' account information. (Subscribers' Obj. at 16); *see Forrester*, 512 F.3d at 510 ("[E]-mail to/from addresses and 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.").

The Subscribers identify no cases holding that Internet users do not voluntarily transmit their IP addresses to the websites they visit, and the government is aware of none. Instead, the Subscribers argue that the magistrate judge should have treated IP addresses as involuntarily conveyed, and therefore distinguishable from the information at issue in *Miller* and *Smith*, because the Third Circuit reached a similar conclusion (albeit in dicta) about cell-site location

information (“CSLI”) in the *Third Circuit Opinion*.<sup>9</sup> 620 F.3d at 317-18. Of course, the *Third Circuit Opinion* is not binding on this Court, and its rationale is contrary to *Smith*’s, 442 U.S. at 745.<sup>10</sup> Further, even the Third Circuit declined to make the analytical leap that the Subscribers now urge – just eight days after issuing the *Third Circuit Opinion*, the Third Circuit concluded that a defendant had voluntarily conveyed his IP address when he visited a website. *See Christie*, 624 F.3d at 574.

Furthermore, as the magistrate judge recognized, Twitter puts its subscribers on notice that it collects their IP address information. (Op. at 13-14). Before a would-be Twitter subscriber can create an account, Twitter informs the subscriber: “By clicking on ‘Create my account’ below, you are agreeing to the Terms of Service above and the Privacy Policy.” (Bringola Decl., Ex. 1, at 2); Twitter Signup page, *available at* <https://twitter.com/signup> (last visited Apr. 4, 2011). The phrase “Privacy Policy” includes a link to the Privacy Policy itself so the prospective subscriber can review it before deciding whether to create an account. *See id.* The Privacy Policy, in turn, explains that Twitter’s servers “automatically record information (‘Log Data’) created by your use of the Services,” and that “Log Data may include information such as your IP address. . . .” Twitter Privacy Policy, *available at* <https://twitter.com/privacy>

---

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

<sup>10</sup>A rationale of the panel majority in the *Third Circuit Opinion* was that users do not expect a carrier to collect CSLI. But under the reasoning in *Smith*, that circumstance is not relevant, since in *Smith* the “fortuity” of “whether or not the phone company in fact elects to make a quasi-permanent record of a particular number dialed” did not make “any constitutional difference.” 442 U.S. at 745. The *Smith* Court emphasized that “[r]egardless of the phone company’s election, petitioner voluntarily conveyed to it information that it had facilities for recording and that it was free to record.” *Id.*

(last visited Apr. 4, 2011). These circumstances provide ample support for the magistrate judge's factual finding - which must be accepted unless clearly erroneous - that the Subscribers "voluntarily conveyed their IP addresses to Twitter as a condition of use." (Op. at 14.)

The Subscribers argue that the magistrate judge erred in citing Twitter's Privacy Policy because, in their view, "the Magistrate inaccurately assumed that users who sign up for Twitter accounts are explicitly notified . . . that IP addresses are collected." (Subscribers' Obj. at 17.) In fact, the magistrate judge did not assume that every user who signs up for a Twitter account actually reads the Privacy Policy. Rather, the Magistrate pointed to the *existence* of the Privacy Policy as further evidence that the Subscribers cannot have an objectively reasonable expectation of privacy in the IP addresses they conveyed to Twitter. (Op. at 13.) Specifically, the magistrate noted that the Privacy Policy existed, and that "readers" of it "are notified that IP addresses are among the kinds of 'Log Data' that Twitter collects, transfers, and manipulates." (Op. at 13.) The magistrate judge's reference to "readers," rather than to all Twitter users or any particular individual, evinced her awareness that not all Twitter users may read the Privacy Policy. But even assuming that the Subscribers had a *subjective* expectation of privacy in their IP addresses,<sup>11</sup> that expectation was not objectively reasonable, and therefore was not protected by

---

<sup>11</sup>Any suggestion that for example Subscriber Jacob Appelbaum, a recognized expert in computer security, was unaware that Twitter users transmit IP addresses to Twitter would strain credulity. Notably, the Subscribers do not assert that they actually failed to read Twitter's Privacy Policy themselves, nor do they claim that they were unaware that they were transmitting their IP addresses to Twitter, or that they subjectively believed that Twitter was not collecting their IP address information. Instead, they argue generally that "research shows that many Internet users do not read the privacy policies for the Internet sites they visit, so it is doubtful that Twitter users would have read such policies, much less understood them." (Subscribers' Obj. at 17.)

the Fourth Amendment. *See Smith*, 442 U.S. at 740 (relevant inquiry is whether “the individual’s expectation, viewed objectively, is ‘justifiable’ under the circumstances”).

The magistrate judge correctly concluded that the existence of the Privacy Policy, even if unread by the Subscribers, undermines the legitimacy of any expectation of privacy the Subscribers may have had in the IP addresses they conveyed to Twitter. Although individual users might be ignorant of the terms of Twitter’s Privacy Policy, society is not prepared to recognize as reasonable an expectation of privacy that is directly contradicted by policy statements available to all who wish to read them. *See* (Op. at 14 n.6 (citing cases)); *Smith v. Maryland*, 442 U.S. at 742-43 (telephone subscribers cannot “harbor any general expectation that the numbers they dial will remain secret” when, among other things, “most phone books tell subscribers . . . that the company ‘can frequently help in identifying to the authorities the origin of unwelcome and troublesome calls’”); *United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000) (government employee “did not have a legitimate expectation of privacy with regard to the record or fruits of his Internet use” on his work computer in light of his employer’s internet policy).

**F. The Magistrate Judge Did Not Abuse Her Discretion in Denying the Subscribers’ Motion to Unseal Additional Court Records.**

Finally, the Subscribers object to the magistrate judge’s denial of their motion to unseal certain court records, on the ground that the government failed to meet its “heavy burden” to keep the records sealed. (Subscribers’ Obj. at 18-29.) As shown below, the Subscribers have failed to establish that the magistrate judge abused her discretion in declining to unseal the records in question.

As the magistrate judge noted, the documents in docket number 1:11-dm-3 (relating directly to the Subscribers' motions) were initially sealed by the Clerk's office, and the Subscribers sought to unseal all of them. (Op. at 16.) Ultimately the parties agreed that sealing was no longer necessary for any of the documents in that docket, except for the original application and two documents (numbers 22 and 24) as to which the government proposed certain minor redactions. (Op. at 16.) The magistrate judge found that the material in document number 22 proposed for redaction "[did] not reveal any sensitive investigatory facts which are not already revealed by the Twitter Order," and directed that document number 22 be released in unredacted form. (Op. at 19.) The magistrate judge also ordered the sole redaction proposed for document number 24 (the email address of a government attorney), and unsealed the redacted version of that document. (Op. at 19.) Thus, as a result of the parties' agreements and the magistrate judge's rulings, every document filed in 1:11-DM-3 was unsealed, except for the government's original application and a prosecutor's email address.<sup>12</sup>

In addition, the Subscribers sought to unseal "all other documents" in case number 10-GJ-3793. (Op. at 16-17.) Further, "to the extent any other companies received similar orders" under § 2703(d), the Subscribers requested the unsealing of those orders and their applications. (Op. at 17.) In support of their claims, the Subscribers invoked both the common law presumption of access to court records, and the First Amendment right of public access. (Op. at 17-18.)

The magistrate judge rejected these additional requests, finding that the Subscribers had no right of access to the sealed documents. The magistrate judge began with the proposition that

---

<sup>12</sup>The Subscribers also sought a public docket with respect to documents filed in 10-GJ-3793. The magistrate judge noted that this request required further review, and took it under consideration. (Op. at 19.)

“[a]t the pre-indictment phase, ‘law enforcement agencies must be able to investigate crime without the details of the investigation being released to the public in a manner that compromises the investigation.’” (Op. at 17 (quoting *Va. Dept. of State Police v. Washington Post*, 386 F.3d 567, 574 (4<sup>th</sup> Cir. 2004).) Magistrate Judge Buchanan noted that in criminal investigations secrecy enhances officer safety; prevents destruction of evidence; protects witnesses against intimidation and retaliation; and preserves the reputations of subjects who are exonerated and never charged. (Op. at 17.)<sup>13</sup> Therefore, she concluded, “sensitive investigatory material is appropriately sealed.” (Op. at 17.)

Turning to the Subscribers’ claim under the common law presumption of openness, the magistrate judge noted that the presumption “may be overcome by a countervailing government interest.” (Op. at 18.) Responding to the Subscribers’ claim that the publicity surrounding the unsealed Twitter Order nullified the traditional reasons for secrecy, the magistrate judge disagreed: “[The Subscribers’] argument ignores the significant difference between revealing the existence of an investigation, and exposing critical aspects of its nature and scope.” (Op. at 18.) Here, the magistrate judge found, “[t]he sealed documents at issue set forth sensitive nonpublic facts, including the identity of targets and witnesses in an ongoing criminal investigation.” (Op. at 18.) She also noted the absence of authority supporting the Subscribers’ argument. The magistrate judge concluded that “[b]ecause the government’s interest in keeping these documents sealed for the time being outweighs [the Subscribers’] interest in accessing them,” there was no common law right of access to the sealed records. (Op. at 18.)

---

<sup>13</sup>Maintaining the confidentiality of criminal investigations has another critical benefit – it helps ensure the integrity of witness statements and testimony. Witnesses cannot fabricate testimony to conform to the facts if they do not know those facts.



The magistrate judge similarly rejected the Subscribers' First Amendment claim to access. She noted that the First Amendment provides a right of access to records "only when (1) the place or process to which access is sought has been historically open to the public, and (2) public access plays a significant positive role in the particular process." (Op. at 19 (citing *Goetz*, 886 F.2d at 63-64).) The magistrate judge concluded that the Subscribers' First Amendment claim failed both prongs of the test, since "there is no history of openness for documents related to an ongoing criminal investigation," and "there are legitimate concerns that publication of the documents at this juncture will hamper the investigatory process." (Op. at 19.)

The Subscribers now raise a fistful of objections to the partial denial of their motion to unseal. First, they assert, the magistrate judge applied the wrong legal tests. (Subscribers' Obj. at 18.) Regarding the common law presumption, they say, the question is not whether the presumption is "overcome by a countervailing government interest," as the magistrate judge framed it (Op. at 18), but rather whether the government has demonstrated that its "countervailing interests *heavily outweigh* the public interests in access." (Subscribers' Obj. at 18 (quoting *Va. Dep't of State Police*, 386 F.3d at 575).) But this is mere quibbling. Whether a countervailing government interest "overcomes" the common law presumption of access, as the magistrate judge stated, or instead "heavily outweighs" it, as the Subscribers (and some cases) put it, is immaterial. Moreover, assuming for argument's sake that the quoted words import different legal standards, the Subscribers have failed to show that the alleged difference affects their "substantial rights," Fed. R. Crim. P. 52(a), in light of the powerful government interest in the confidentiality of pre-indictment investigations, *see ACLU v. Holder*, — F.3d —, 2011 WL 1108252, at \*7 (4<sup>th</sup> Cir. 2011) ("The United States has a compelling interest in protecting the

integrity of ongoing fraud investigations”), and the dearth of authority (Op. at 18) supporting their claim to a right of access.

The Subscribers also complain that in rejecting their First Amendment claim to access the magistrate judge failed to undertake a proper “logic” analysis, and “ignored the positive role that openness regarding the § 2703 proceedings would serve.” (Subscribers’ Obj. at 19.) The unsealing of the Twitter Order, according to the Subscribers, provides one example of the “positive role” of “openness,” since, “had the Twitter Order not been unsealed, the Parties and the public would never have known its breadth, and they would have been unable to mount a challenge to protect their constitutional rights.” (Subscribers’ Obj. at 19.) But this argument improperly assumes that the Order would never have been unsealed, even after the present investigation concludes, and that the Subscribers would be powerless to defend their rights in any later proceedings. More to the point, if the present litigation – in which, at great expense to the public, and in the face of a clear statutory mandate, the Subscribers have delayed for at least four months a routine step in a legitimate criminal investigation so that they may argue and press on appeal multiple constitutional and statutory claims for which no authority exists and which are (at least thus far) roundly and uniformly rejected – constitutes the Subscribers’ prime example of the “positive” benefits *to the public* of uniformly open § 2703 proceedings in pre-indictment settings, we are not convinced -- and the magistrate judge would not have been either.<sup>14</sup> No nuanced “logic” analysis was required to grasp the commonsense point here: that

---

<sup>14</sup>The Supreme Court has recognized the public’s countervailing interest in the expeditious administration of criminal law and the production of relevant evidence. *See Zurcher v. Stanford Daily*, 436 U.S. 547, 560-62 n. 8 (1970) (recognizing the fundamental public interest in implementing the criminal law and rejecting notion that Fourth Amendment requires subpoena *duces tecum* as opposed to search warrant for third parties, since delay resulting from litigation of subpoenas could result in disappearance of evidence and time spent litigating “could seriously impede criminal investigations”), *but cf.* 42 U.S.C. § 2000aa; *United States v. Nixon*, 418 U.S.

law enforcement agents must be able to investigate an alleged crime without the details of the investigation being released to the public in a manner that compromises the investigation. (Op. at 17.)

The Subscribers also contend that the unsealing of the Twitter Order removed any justification for continued sealing of the documents in question. (Subscribers' Obj. at 21.) But, as the magistrate judge correctly observed, the Subscribers continue to ignore the signal distinction between revealing the fact of an investigation "and exposing critical aspects of its nature and scope." (Op. at 18.) Here, although the fact of the investigation is public, the application for the Order remains sealed, and properly so. Such an application, of course, cannot be *pro forma*; it must necessarily describe "specific and articulable facts" showing "reasonable grounds to believe" that the records sought are "relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). Thus, an application to a court under the statute must describe a criminal investigation; must articulate specific facts; and must show that the information sought is relevant and material to the case. Depending on the level of detail required, an application may summarize the investigation's history; identify targets, witnesses, and cooperating witnesses; summarize key documents, witness statements, or forensic tests; and explain the significance of items of evidence. Here, notwithstanding the public nature of the Twitter Order, the magistrate judge expressly found that the unsealing of the remaining

---

683, 690-91, 713 (1974) (discussing that finality requirement embodies congressional policy against impeding ongoing judicial proceedings and necessity for expedition in the administration of criminal law; further, in rejecting general claim of confidentiality privilege against subpoena, explaining that "the constitutional need for production of relevant evidence in a criminal proceeding is specific and central to the fair adjudication of a particular criminal case in the administration of justice. Without access to specific facts a criminal prosecution may be totally frustrated").

documents would reveal “sensitive nonpublic facts, including the identity of targets and witnesses.” (Op. at 18.) That finding cannot be shown to be clearly erroneous. *See Va. Dep’t of State Police*, 386 F.3d at 579 (in deciding whether an asserted interest is compelling, noting that one consideration is “whether the granting of access to the contents of an ongoing police investigation file will disclose facts that are otherwise unknown to the public”).

The Subscribers also maintain that the magistrate judge erred in failing to consider their significant interests in unsealing the documents in question. (Subscribers’ Obj. at 22.) They state that continued sealing would “frustrate [their] ability to exercise their right to challenge the § 2703 orders.” (Subscribers’ Obj. at 23.) But, as demonstrated *supra*, the Subscribers have no standing to challenge the § 2703(d) Order; can identify no valid statutory or constitutional basis to vacate it; and can only speculate about whether additional hypothetical orders exist. In these circumstances, and in light of the loss of privacy that may flow from public disclosure of investigative details, it is not at all clear that the Subscribers’ interests lie in unsealing. In any event, they have not shown that the magistrate judge abused her discretion in assessing their interests.

Next the Subscribers assert that the magistrate judge ignored the public’s interest in obtaining access to the sealed documents. (Subscribers’ Obj. at 24.) But the magistrate judge did not ignore the public’s interest – she recognized it, but determined that “for the time being” it was outweighed by the government’s interest in the confidentiality of its investigation. (Op. at 18.) The magistrate judge thus properly acknowledged that with respect to sealing and unsealing timing is critical. (Op. at 18 (citing *In the Matter of Application and Affidavit for a Search Warrant*, 923 F.2d 324, 326 (4<sup>th</sup> Cir. 1991) (affirming decision to unseal affidavit only after investigation had concluded); *see ACLU v. Holder*, 2011 WL 1108252, at \*12 (recognizing that

“Congress has determined that temporary confidentiality can assist the functioning of certain processes”). The public has a vital interest in access to judicial documents in criminal cases – but, in many cases, while the investigation is ongoing that interest is “heavily outweighed” by the interest in confidentiality.

The Subscribers further protest that the “generic” interests in secrecy supposedly offered by the government are insufficient. (Subscribers’ Obj. at 25.) But the claim that the government offered only boilerplate pabulum to the magistrate is demonstrably false. The government filed an application under § 2703(d) containing specific facts. In denying the Subscribers’ motion to unseal, the magistrate judge expressly found that “[t]he sealed documents at issue set forth sensitive nonpublic facts, including the identity of targets and witnesses in an ongoing criminal investigation.” (Op. at 18.) Thus, in assessing the need to maintain confidentiality, the magistrate judge reviewed specifics, not generalities, assessed for herself the relative costs and benefits of unsealing at this stage of the case, and made her findings. Nothing more was required, and no abuse of discretion occurred. *Media General Operations, Inc.*, 417 F.3d at 430 (declining to adopt blanket rule that sealing order “must be accompanied by a separate order detailing why sealing is appropriate,” and finding that magistrate judge’s reasons for sealing and rejecting alternatives to sealing were “patently apparent from the affidavits”).

The Subscribers also complain that the magistrate judge erred by not expressly ruling on whether each specific document at issue, including the hypothetical “§ 2703 orders to other companies,” should remain sealed. (Subscribers’ Obj. at 27.) But the magistrate judge did individually review the only two documents (and the accompanying proposed redactions) at issue in 1:11-dm-3, and made specific findings. (Op. at 19.) The magistrate judge also necessarily considered and rejected the Subscribers’ argument for unsealing of the application.

*See* (Op. at 16.) But these individualized findings with respect to known documents were insufficient, say the Subscribers, because the magistrate judge did not go on to require the government to explain “why any similar orders to other companies should remain unsealed.” (Op. at 27.)

The Subscribers thus predicate a claim of error on sheer speculation – their conjecture that similar § 2703 orders must have been directed to businesses other than Twitter. They also impliedly assert that they have standing to file challenges in this Court to judicial orders about which they do not know and which may not exist. And they claim entitlement to a judicial explanation as to why “orders to other companies” – if they exist – are under seal, even though the magistrate judge in giving such an explanation would necessarily violate the sealing order and eviscerate the reason for sealing in the first place. Such a legal position is preposterous, and the magistrate judge did not abuse her discretion in rejecting it.

Finally, the Subscribers object that the magistrate judge improperly failed to consider alternatives to sealing. (Subscribers’ Obj. at 28.) But her reasons for rejecting alternatives to sealing the affidavit are “patently apparent” from the Opinion and from the affidavit itself, and no separate explanation was required. *Media General Operations, Inc.*, 417 F.3d at 430. In light of the flexibility afforded magistrate judges in *Media General Operations, Inc.*, the Subscribers’ reliance upon earlier and more exacting Fourth Circuit cases is unavailing.

#### **IV. Conclusion**

For the reasons stated, this Court should overrule the Subscribers’ objections to the magistrate judge’s Memorandum Opinion and Order of March 11, 2011, and direct Twitter to fully and promptly comply with the Order and the magistrate judge’s related rulings.

Respectfully submitted,

Neil H. MacBride  
United States Attorney

By: \_\_\_\_\_/s/\_\_\_\_\_  
John S. Davis  
Tracy Doherty-McCormick  
Andrew Peterson  
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 Response was filed with the Clerk of the Court on April 8, 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](mailto: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](mailto: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](mailto: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](mailto:rglenberg@acluva.org)  
Counsel for Birgitta Jonsdottir

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