

FILED

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

2011 FEB 10 P 4:42
CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA
J

IN RE APPLICATION OF THE UNITED
STATES OF AMERICA FOR AN ORDER
PURSUANT TO 18 U.S.C. §2703(d)

MISC NO. 10GJ3793, 1:11-DM-003

**REPLY IN SUPPORT OF MOTION OF REAL PARTIES IN INTEREST JACOB
APPELBAUM, ROP GONGGRIJP AND BIRGITA JONSDOTTIR TO VACATE
DECEMBER 14, 2010 ORDER**

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. ARGUMENT.....	2
A. The Parties have a right to be heard.....	2
B. The Order should be vacated because the Government cannot show that the records sought are “relevant and material to an ongoing criminal investigation.”.....	4
C. This Court should exercise its discretion under the statute and vacate the Order.	6
D. The Court should vacate the Order to preserve Fourth Amendment rights.	9
E. The Court should vacate the Order to preserve important First Amendment freedoms.....	16
F. The Court should vacate the Order as to Ms. Jonsdottir due to International Comity.....	19
III. CONCLUSION.....	20

TABLE OF AUTHORITIES

Page(s)

Federal Cases

<i>American-Arab Anti-Discrimination Committee v. Reno</i> 70 F.3d 1045 (9th Cir. 1995)	3
<i>Brandenburg v. Ohio</i> 395 U.S. 444 (1969)	18
<i>California v. Hodari D.</i> 499 U.S. 621 (1991)	6
<i>City of Lakewood v. Plain Dealer Publishing Co.</i> 486 U.S. 750 (1988)	17
<i>Cooter & Gell v. Hartmarx Corp.</i> 496 U.S. 384 (1990)	8
<i>Eastland v. U.S. Servicemen's Fund</i> 421 U.S. 491 (1975)	2
<i>Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.</i> 528 U.S. 167 (2000)	17
<i>Gunnells v. Healthplan Servs., Inc.</i> 348 F.3d 417 (4th Cir. 2003)	5
<i>Gutierrez de Martinez v. Lamagno</i> 515 U.S. 417 (1995)	7
<i>Hecht Co. v. Bowles</i> 321 U.S. 321 (1944)	7
<i>Hilton v. Guyot</i> 159 U.S. 113 (1895)	20
<i>In re Application of U.S. for an Order Directing a Provider of Elec. Comm'n Serv. to Disclose Records to Gov't,</i> 620 F.3d 304 (3d Cir. 2010)	<i>passim</i>
<i>In re Application of the United States</i> 632 F. Supp. 2d 202 (E.D.N.Y. 2008)	9
<i>In re French</i> 440 F.3d 145 (4th Cir. 2006)	20
<i>In re Grand Jury Subpoena: SDT</i> 829 F.2d 1291 (4th Cir. 1987)	18, 19
<i>In re: Grand Jury 87-3 Subpoena Duces Tecum</i> 955 F.2d 229 (4th Cir. 1992)	18
<i>Joint Anti-Fascist Committee v. McGrath</i> 341 U.S. 123 (1951)	3
<i>Katz v. United States</i> 389 U.S. 347 (1967)	13
<i>Kyllo v. United States</i> 533 U.S. 27 (2001)	10, 12, 14
<i>Lamont v. Woods</i> 948 F.2d 825 (2d Cir. 1991)	9

TABLE OF AUTHORITIES
(cont'd)

	<u>Page(s)</u>
<i>Mathews v. Eldridge</i> 424, U.S. 319 (1976)	3
<i>Miller-El v. Cockrell</i> 537 U.S. 322 (2003)	7
<i>NAACP v. Button</i> 371 U.S. 415 (1963)	17
<i>Rafeedie v. INS</i> 880 F.2d 506 (D.C. Cir. 1989).....	3
<i>Smith v. Maryland</i> 442 U.S. 735 (1979)	11, 12, 13, 15
<i>Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court</i> 482 U.S. 522 (1987)	20
<i>Stone v. INS</i> 514 US 386 (1995)	5
<i>Terry v. Ohio</i> 392 U.S. 1 (1968)	5
<i>Township of Tincum v. U.S. Dep't of Transp.</i> 582 F.3d 482 (3d Cir. 2009)	7
<i>Triton Marine Fuels Ltd., S.A. v. M/V PACIFIC CHUKOTKA</i> 575 F.3d 409 (4th Cir. 2009).....	6
<i>United States v. Bynum</i> 604 F.3d 161 (4th Cir. 2010).....	15
<i>United States v. Christie</i> 624 F.3d 558 (3d Cir. 2010)	15
<i>United States v. Forrester</i> 512 F.3d 500.....	15
<i>United States v. Inigo</i> 925 F.2d 641 (3d Cir. 1991)	9
<i>United States v. Karo</i> 468 U.S. 705 (1984)	passim
<i>United States v. Mason</i> 628 F.3d 123 (4th Cir. 2010)	5
<i>United States v. Maynard</i> 615 F.3d 544 (D.C. Cir. 2010),	9, 12, 13, 16
<i>United States v. Miller</i> 425 U.S. 435 (1976)	11
<i>United States v. N.Y. Tel. Co.</i> 434 U.S. 159 (1977)	13
<i>United States v. Verdugo-Urquidez</i> 494 U.S. 259 (1990)	9
<i>United States v. Wanigasinghe</i> 545 F.3d 595 (7th Cir. 2008).....	9

TABLE OF AUTHORITIES
(cont'd)

	<u>Page(s)</u>
<i>United States v. Warshak</i> No. 08-3997, ___ F.3d ___, 2010 WL 5071766 (6th Cir. Dec. 14, 2010)	14, 16
<i>Virginia v. Am. Booksellers Ass'n, Inc.</i> 484 U.S. 383 (1988)	17
<i>Wang v. Reno</i> 81 F.3d 808 (9th Cir. 1996)	9
Federal Statutes	
18 U.S.C. § 2703	2, 7
18 U.S.C. § 2703(c)(1)(A)	8
18 U.S.C. § 2703(d)	<i>passim</i>
18 U.S.C. § 2704	4
18 U.S.C. § 2704(a)(2)	2
18 U.S.C. § 2704(b)	4
18 U.S.C. § 2704(b)(1)	3
18 U.S.C. § 2704(b)(1)(B)	4
18 U.S.C. § 2707(a)	3
18 U.S.C. § 2708	2
18 U.S.C. § 2712(a)	3
18 U.S.C. § 3123(a)	7
18 U.S.C. § 3123(a)(1)	7
18 U.S.C. § 3127(2)(A)	8
Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat 4279, Title II, § 207(a)(2)	8
Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, Title II, 100 Stat 1848, § 201	7
USA PATRIOT Act of 2001, Pub.L. 107-56, Title II, 115 Stat. 272, § 220(b)	8
Federal Rules	
Federal Rules of Criminal Procedure § 41(d)(1)	8
Constitutional Provisions	
Debate Clause of the U.S. Constitution	19
First Amendment	1, 16, 17, 18, 19
Fourth Amendment	<i>passim</i>
Other Authorities	
Joseph Turow, Americans & Online Privacy, The System is Broken, Annenberg Public Policy Center (June 2003)	14

I. INTRODUCTION

The Government's arguments here present a troubling picture of the privacy rights of individuals in the digital age. In its view, a person who learns about an upcoming disclosure of detailed electronic records related to her speech activities cannot act to protect her rights before disclosure, regardless of the disclosure demand's legality or constitutionality, its overbreadth, or the harm that may come from it, unless she can show that the government is intentionally harassing her. In the Government's view, an order issued after hearing only from the Government cannot later be modified based on consideration of facts and legal argument presented in an adversarial process. In its view, the "materiality" requirement for § 2703(d) orders is just for show, and not enforceable by the parties actually affected by an order. In its view, the fact that Twitter is a vehicle for publication means that the non-public records it keeps about speakers are unprotected by the First Amendment, and IP addresses, which can be used to track individuals' locations while they are engaged in speech activity and which are involuntarily and invisibly recorded by services like Twitter, lose the protection afforded for other location tracking mechanisms like beepers and GPS. And, in the Government's view this Court cannot require any more than mere "specific and articulable facts" even if a governmental request raises serious constitutional questions.

The Government is wrong. Users of online services who learn of governmental efforts to obtain tracking information about them have the right to act to prevent such disclosures. Courts can consider adversarial presentations about whether the legal and constitutional standards limiting such efforts have been met, including § 2703's materiality requirement, even if a disclosure order has already issued. Users of online service retain privacy interests in non-public records related to their speech activities and when those records can be used to track them, including into their homes, the proper legal standards are those applicable to other tracking devices. Finally, because important constitutional are questions raised by the Government's request, the Court has discretion to require the Government to meet the more rigorous standards applicable to search warrants.

Given the serious questions raised here about the Government's showing and the

constitutional issues raised by its request, the Government's Order should be vacated.

II. ARGUMENT

A. The Parties have a right to be heard.

The Government claims that the Court should not even entertain the Parties' motion to vacate¹ because § 2708 of the Stored Communications Act ("SCA") limits available remedies, and the Act does not explicitly permit subscribers to challenge orders unless they require disclosure of the content of stored communications. Obj.² at 4-6. The Court should reject the Government's effort to deny Parties an opportunity to be heard.

First, as the Parties explained in their moving papers, courts have regularly recognized an aggrieved party's right to challenge disclosure of the party's information upon notice of the impending discovery. *See* Mtn. at 9; *see, e.g., Eastland v. U.S. Servicemen's Fund*, 421 U.S. 491, 501 n.14 (1975) (individuals must have right to challenge third-party subpoena for their records or unconstitutional intrusions could go unchallenged). The Government does not even address—much less overcome—this authority. The Government also does not explain why challenges to § 2703 orders should be treated any differently. Where, as here, an individual's constitutional rights are at stake, that person must have the right to bring an immediate challenge to government snooping.

Second, while the SCA does not specifically provide for a motion to quash non-content disclosure orders, that is because the subscriber or customer typically will not get notice of the order in the first place. But the statute's tolerance of records requests without notice to the aggrieved party is no reason to deny that party a chance to challenge disclosure where, as here, the aggrieved party is notified of a disclosure order. *See Eastland*, 421 U.S. at 501 n.14 (recognizing right of non-subpoenaed party to challenge subpoena that implicates his interests). Indeed, where the SCA provides for notice to the aggrieved party, it also permits that party to file

¹ Motion Of Real Parties In Interest Jacob Appelbaum, Birgitta Jonsdottir, and Rop Gonggrijp To Vacate December 14, 2010 Order (hereinafter "Motion" or "Mtn.").

² Government's Objection to Motion of Three Twitter Subscribers to Vacate Order of December 14, 2010, under § 2703(d) (hereinafter "Objection" or "Obj.").

a motion to quash any disclosure order.³ Moreover, a person harmed can file a civil action for willful violations of the SCA, including against the United States *See* 18 U.S.C. §§ 2707(a) and 2712(a).

Thus, the SCA specifically contemplates that individuals whose records may be disclosed have remedies for improper disclosure, and Congress clearly contemplated motions to quash by aggrieved parties that have notice of such orders. It makes no sense to permit an aggrieved party to file a civil suit for violations of the SCA without first affording him an opportunity to prevent that violation from happening. Indeed, in the civil context, plaintiffs have an obligation to mitigate damages, and attempts to prevent the harm in the first instance (when one knows about it) are classic mitigation efforts that should not be so readily rejected. Moreover, the United States does not lightly waive its civil immunity, so Congress could not have intended to open the sovereign purse without also providing for the lesser remedy of a motion to quash that might remedy any harm at the outset.

Third, the very foundation of our legal system is based on an adversary system which ensures that persons whose rights are affected have the opportunity to be heard and challenge government action. As Justice Frankfurter long ago cautioned, “democracy implies respect of the elementary rights of men...[and] must therefore practice fairness; and fairness can rarely be obtained by secret, one-sided determination of facts decisive of rights.” *Joint Anti-Fascist Committee v. McGrath*, 341 U.S. 123, 170 (1951) (Frankfurter, J., concurring). Fundamental fairness demands that the Parties have the right to challenge disclosure of their records here. *See, e.g., American-Arab Anti-Discrimination Committee v. Reno*, 70 F.3d 1045, 1068-71 (9th Cir. 1995) (rejecting use of secret evidence in deportation proceedings); *Rafeedie v. INS*, 880 F.2d 506, 524-25 (D.C. Cir. 1989) (applying due process balancing test for exclusion proceedings and use of secret evidence, emphasizing that “the fundamental requirement of due process is the opportunity to be heard ‘at a meaningful time and in a meaningful manner’”) (quoting *Mathews*

³ Section 2704(a)(2) provides that “the subscriber or customer” will receive notice of an order to disclose content of communications in certain circumstances. After such notice, the aggrieved party “may file a motion to quash such subpoena or vacate such court order.” 18 U.S.C. § 2704(b)(1).

v. Eldridge, 424, U.S. 319, 333 (1976)).

For these reasons, the Court can, and should, entertain the Parties' motion to vacate the December 14, 2010 order requiring disclosure of their Twitter information.

B. The Order should be vacated because the Government cannot show that the records sought are "relevant and material to an ongoing criminal investigation."

The Government insists that the Parties argue in a vacuum—denying them access to the Application—and then blithely dismisses the Parties' complaints by proclaiming them baseless and insisting that the Application is perfectly fine, merely because the Government says so. In so doing, the Government tries to read the "materiality" requirement out of § 2703(d) altogether, claiming a right to demand disclosure with the most minimal and insufficient of showings.

The Government argues that, even if the Parties can file motions to quash, the Order at issue must be sufficient because the Government does not need to show that the Parties' information sought is material to an investigation. *See* Obj. at 6, n.3. The Government makes this argument even though § 2703(d) explicitly requires a showing that "the records or other information sought, are [both] relevant and material to an ongoing criminal investigation." (emphasis added). The Government seeks to evade § 2703's plain language by claiming that a "materiality" showing is not required since § 2704, the only SCA section discussing a customer's motion to quash orders, provides a lower bar for disclosure. The Government is wrong, as it simply ignores the full text of § 2704(b).

Under § 2704(b)(1)(B), a customer challenging a disclosure order must show that "the records sought are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this chapter in some other respect" (emphasis added). Here, this "in some other respect" language that the Government ignores goes directly to § 2703(d)'s requirement that the information sought must be "relevant and material to an ongoing criminal investigation." If the Government's application does not establish both relevance and materiality, it is not in "substantial compliance with the provisions of [§ 2703(d)]" and should be quashed.

The Government also cannot be allowed to read the "materiality" requirement out of

§ 2703(d) because doing so would, in the Government's own words, "violate[] 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.'" Obj. at 23 (quoting *Gunnells v. Healthplan Servs., Inc.*, 348 F.3d 417, 439-40 (4th Cir. 2003)). And where, as here, the Government notes that the "materiality" term was added by Congress in 1994 (Obj. at 6, n. 3), such argument also violates the general presumption that, when Congress alters the words of a statute, it must intend to change the statute's meaning. See *Stone v. INS*, 514 US 386, 397 (1995) ("When Congress acts to amend a statute, we presume it intends its amendment to have real and substantial effect"). The Order is subject to challenge based on whether the Government met § 2703's materiality requirement.

As the Parties explained in their moving papers, where proof of materiality is required, courts demand a showing beyond mere speculation, a showing that the information sought is "vital" or "highly relevant" to the inquiry or "helpful" or "essential" to the party's position. See Mtn. at 5 (citing cases). The Government offers no alternative meaning of § 2703(d)'s "material" element and fails to distinguish the authorities cited in the Parties' motion.

The Government also seeks refuge in a *Terry v. Ohio*, 392 U.S. 1 (1968) "specific and articulable facts" standard (Obj. at 8-9), but that does not rescue its Application here. First, this argument ignores the plain language of § 2703(d), which requires a "relevant and material" showing. Second, as the Government acknowledges, even *Terry* demands a showing of specific and articulable facts that "evinced more than an inchoate and unparticularized suspicion or hunch of criminal activity." Obj. at 8 (quoting *United States v. Mason*, 628 F.3d 123, 128 (4th Cir. 2010)). Here, the Government's Application appears based directly on an "unparticularized suspicion or hunch" that the Parties' Twitter records sought have some connection to its investigation of WikiLeaks. This cannot be the case—the vast majority of the Parties' Twitter activity has nothing to do with the WikiLeaks website. See Mtn. at 4.

In sum, the Government's arguments regarding the "materiality" standard should be denied – the Order should be vacated as it fails to meet § 2703's standards.

C. This Court should exercise its discretion under the statute and vacate the Order.

As the Third Circuit recently held, 18 U.S.C. § 2703(d) provides courts with the discretion to deny applications for orders under that section even when the Government has made the required “specific and articulable facts” showing. *See In re Application of U.S. for an Order Directing a Provider of Elec. Commc’n Serv. to Disclose Records to Gov’t*, 620 F.3d 304, 315-17 (3d Cir. 2010) (hereinafter “*Third Circuit Opinion*”), *pet. for reh’g en banc denied* (3d Cir. Dec. 15, 2010). In response, the Government repeats the same arguments that were persuasively rejected in the *Third Circuit Opinion*. As detailed below, this Court has the discretion under the statute to deny—or, in this case, vacate—the issuance of § 2703(d) orders and instead require the Government to seek a probable cause warrant. The Court must exercise that discretion in cases where to do otherwise would require a court to unnecessarily resolve serious constitutional questions. This is such a case.

Every exercise of statutory interpretation begins with an examination of the statute’s plain language, and where statutory language is “plain and unambiguous,” no further inquiry is necessary. *Triton Marine Fuels Ltd., S.A. v. M/V PACIFIC CHUKOTKA*, 575 F.3d 409, 416 (4th Cir. 2009) (quotation omitted). Section 2703(d)’s plain language provides that:

A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

18 U.S.C. § 2703(d) (emphasis added).

As the Third Circuit panel unanimously held, Congress’ instruction that the court shall issue an order “only if” the Government makes the requisite showing also grants courts discretion to deny a government application even when that showing has been made. *See Third Circuit Opinion*, 620 F.3d at 315-17, 319; *see also id.* at 320-21 (Tashima, J., concurring) (agreeing with the majority that statute provides discretion, though disagreeing on the scope of that discretion). This straightforward holding—that the “only if” in § 2703(d) states a necessary but not sufficient condition for the issuance of a § 2703(d) order—flows directly from Supreme

Court precedent. *See id.* at 316, citing *California v. Hodari D.*, 499 U.S. 621, 627-8 (1991) (“only if . . . states a *necessary*, but not a *sufficient*, condition. . . .”) (emphasis in original); accord *Miller-El v. Cockrell*, 537 U.S. 322, 349 (2003); *Township of Tinicum v. U.S. Dep’t of Transp.*, 582 F.3d 482, 488 (3d Cir. 2009) (“The phrase ‘only if’ describes a necessary condition, not a sufficient condition.”). By choosing the phrase “only if” rather than simply “if” in § 2703(d), Congress made clear that a court may issue, but is not required to issue, a § 2703(d) order when the Government has made a specific and articulable facts showing. Section 2703(d)’s plain meaning is made all the clearer by comparison to the Pen Register Statute’s mandatory language, which contains no “only” and provides that a court “shall enter [an order for pen register surveillance] if” the Government makes the required certification. *See* 18 U.S.C. § 3123(a)(1). As the *Third Circuit Opinion* correctly noted, reading § 2703(d)’s “shall” as a command rather than a permission would render “only” surplusage: “[T]he difference between ‘shall...if’ [in § 3123(a)]... and ‘shall...only if’ [in § 2703(d)]... is dispositive.” *Third Circuit Opinion*, 620 F.3d at 316.

That Congress chose to use the phrase “shall issue” rather than the more obviously permissive “may issue” does not change the discretionary nature of the provision. Although the Government flatly claims that “shall” is “language of command” (Obj. at 23), the Supreme Court has long recognized that Congress often uses “shall” as a synonym for “may”: “‘Shall’ and ‘may’ are frequently treated as synonyms and their meaning depends on context...courts in virtually every English-speaking jurisdiction have held-by necessity-that shall means may in some contexts, and vice versa.” *Gutierrez de Martinez v. Lamagno*, 515 U.S. 417, 432 n.9 (1995) (internal citations and quotations omitted) (reading “shall” as “may”); *see also Hecht Co. v. Bowles*, 321 U.S. 321, 329 (1944) (same). Read in context as the Supreme Court has instructed, the “shall” in § 2703(d)—when paired with the clearly permissive phrase “only if”—must itself be permissive. Indeed, it can be read in no other way without reading the word “only” out of the statute.⁴ As the Third Circuit found, “[t]he difficulty with the Government’s

⁴ The Government ignores the SCA’s history when it claims that Congress’ use of “may” elsewhere in § 2703(d) requires an opposite conclusion. Obj. at 23. The portion of § 2703(d)

argument is that the statute does contain the word ‘only’ and neither we nor the Government is free to rewrite it.” *Third Circuit Opinion*, 620 F.3d at 316.

The Government’s fears that a plain language reading of § 2703(d) “would permit a magistrate judge to arbitrarily deny an application” or even “reject a § 2703(d) order even if the government established probable cause” are based on misunderstandings of both the scope of the court’s discretion and the structure of the statute. First, the magistrate’s discretion is of course not boundless: “[N]o judge in the federal courts has *arbitrary* discretion” *Id.* at 320 (emphasis added). Rather, a magistrate’s decision to require a warrant “must be supported by reasons” justifying a divergence from § 2703(d)’s “specific and articulable facts” standard. *Id.* at 316-17. In other words, courts clearly may not *abuse* the discretion that has been granted to them. Rather, a court must have a sound reason to support its use of discretion—for example, the avoidance of serious constitutional questions. *See Cooter & Gell v. Hartmarx Corp.*, 496 U.S. 384, 405 (1990).

Second, a court has discretion under § 2703(d) only to grant or deny the Government’s application for a § 2703(d) order based on a specific and articulable facts showing. Nothing in the statute’s language or the *Third Circuit Opinion*’s reasoning provides courts with permission to fashion an alternative standard for such an order. If a court uses its discretion to deny a § 2703(d) application despite a “specific and articulable facts” showing by the Government, then the Government may seek a warrant via § 2703(c)(1)(A) under the Federal Rules of Criminal Procedure, which requires probable cause. *See Fed. R. Crim. P. 41(d)(1)*. The Government’s fears of a judiciary gone wild with discretion are therefore unfounded.

that clarifies which courts have authority to issue orders under that section—in particular, the phrase “may be issued by any court that is a court of competent jurisdiction and”—did not exist in the original statute but rather was added in 1994. *Compare* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, Title II, 100 Stat 1848, § 201 (establishing § 2703) *and* Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat 4279, Title II, § 207(a)(2) (amending § 2703(d) to add clause regarding jurisdiction); *see also* USA PATRIOT Act of 2001, Pub.L. 107-56, Title II, 115 Stat. 272, § 220(b) (striking “described in section 3127(2)(A)” after “court of competent jurisdiction”). The “may be issued” language that the Government argues makes surplusage of the panel’s reading of “shall” was added later, and the different clauses were clearly intended to serve different functions. Because one specifies which courts have jurisdiction to issue § 2703(d) orders and the other defines the necessary, though not necessarily sufficient, condition for issuance of such an order, neither is

Finally, the Government contends that the doctrine of constitutional avoidance does not require this Court to adopt the discretionary reading of § 2703(d), claiming that Parties have failed to raise any serious constitutional questions and making the novel suggestion that constitutional avoidance doctrine does not apply to statutes governing search and seizure. Obj. at 24 (citing *In re Application of the United States*, 632 F. Supp. 2d 202, 210 (E.D.N.Y. 2008)). But, that doctrine does not control where the statute's language is plain, and the statute here plainly gives courts the discretion to deny the Government's applications. Nor should this Court be swayed by a single district court's holding, without citation to any precedent, that statutes raising Fourth Amendment questions are somehow carved out of the constitutional avoidance doctrine. As demonstrated further below, it is clear that the Order at issue here raises serious questions under both the First and Fourth Amendments.

D. The Court should vacate the Order to preserve Fourth Amendment rights.

Under established U.S. law, the Parties have a Fourth Amendment reasonable expectation of privacy in information revealing their, or their effects', locations in private spaces, and information revealing the sum of their public movements between private spaces over extended periods of time.⁵ See *United States v. Karo*, 468 U.S. 705, 714-16 (1984); *United States v. Maynard*, 615 F.3d 544, 559 (D.C. Cir. 2010), *pet. for reh'g en banc denied* (D.C. Cir. Nov. 19,

surplus to the other.

⁵ The Government suggests that the First and Fourth Amendments do not apply to Ms. Jonsdottir and Mr. Gonggrijp because they are non-citizens residing abroad. Obj. at 10-11 n.4 (citing *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990)). This incorrect. As several courts have correctly recognized, *Verdugo-Urquidez*'s holding addresses only extraterritorial searches and seizures. See, e.g., *United States v. Wanigasinghe*, 545 F.3d 595, 597 (7th Cir. 2008); *Lamont v. Woods*, 948 F.2d 825, 834 (2d Cir. 1991); *United States v. Inigo*, 925 F.2d 641, 656 (3d Cir. 1991). The § 2703(d) Order here was issued by a United States court and directed at information stored in the United States; hence, the Constitution governs the order, and *Verdugo* does not apply. See, e.g., *Wang v. Reno*, 81 F.3d 808, 817-20 & n.16 (9th Cir. 1996) (rejecting the government's *Verdugo* argument that a foreign individual could not assert a due process violation based on government actions taken within the United States because those actions had occurred when he was not present here); *Lamont*, 948 F.2d at 834 (contrasting the Fourth Amendment violation in *Verdugo*, which was "fully accomplished at the time of the unreasonable governmental intrusion" and hence "occurred solely in Mexico," with the Establishment Clause violation alleged in *Lamont*, which would have occurred "in the United States" at the time money was granted, and not "at the time the money was received or expended" abroad). The Government's action here, like the actions in *Wang* and *Lamont* and unlike the actions in *Verdugo*, occurred entirely within the United States. The First and Fourth Amendments squarely apply.

2010). As IP logs such as those sought from Twitter reveal such Fourth Amendment-protected location information, the Government's search or seizure of the logs requires probable cause.

In claiming that the IP logs cannot be protected under *Karo*, the Government misconstrues that case and ignores later Supreme Court precedent. The Government claims that *Karo* only protects "critical facts" about the interior of a private home, and does not protect against the Government obtaining "more generalized" information. Obj. at 19. However, "[t]he Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained." *Kyllo v. United States*, 533 U.S. 27, 37-38 (2001). Fourth Amendment protection does not hinge on whether the information revealed is an "intimate detail." *Id.* Rather, even information that does not directly reveal but only enables the inference of facts about the interior of a home "falls within the ambit of the Fourth Amendment when it reveals information that could not have been obtained through visual surveillance." *Karo*, 468 U.S. at 707; *see also Kyllo*, 533 U.S. at 36 (rejecting the "novel proposition that inference insulates a search," which is "blatantly contrary" to *Karo*).

Twitter's IP log information, on the other hand—even where it only directly reveals location to within a 25 mile radius (Obj. at 20)⁶—allow one to infer, in combination with knowledge of a person's home and office addresses, that the person was inside her home or office using Twitter at the logged times. These inferences are made even stronger when logs reveal which IP addresses were used most consistently within that 25 mile radius, and whether they were used during business or personal hours. More importantly, when combined with IP address assignment logs from an Internet Service Provider, the requested records may directly reveal the exact location of the home or office using that Internet connection – no inference is needed. *See Mtn.* at 11. Such information falls squarely within *Karo* and *Kyllo*'s protections. *See Third Circuit Opinion*, 620 F.3d at 312-13.

⁶ Under both *Karo* and *Kyllo*, protected location information does not need to be so precise as to pinpoint the location of an item or person in the home, so long as that information, in combination with reason or with other facts, generates inferences about the home's interior. Certainly, it need not be so precise as to identify the particular storage locker in which an item is stored, as the Government implies in its recounting of *Karo*. Obj. at 20. In *Karo*, there was no way for the police to infer based on the tracking information which private locker the ether being

To avoid this conclusion, the Government also tries to analogize the IP log information at issue here with the dialed phone number information that the Supreme Court found was unprotected by the Fourth Amendment in *Smith v. Maryland*, 442 U.S. 735 (1979) and *United States v. Miller*, 425 U.S. 435 (1976). This argument fails, however, because *Smith* and *Miller* do not support the broad proposition that one may never have an expectation of privacy in another's "business records." Instead, as the Supreme Court made clear in *Miller*, the conclusion that Miller's information was unprotected by the Fourth Amendment turned not on the fact that the bank owned or possessed the records, but on the fact that Miller "knowingly expose[d]" and "voluntarily conveyed" their contents to the bank. *Miller*, 425 US at 440, 442 (noting that "[w]e must examine the nature of the particular documents...to determine whether there is a legitimate 'expectation of privacy' concerning their contents.") (internal quotation marks and citation omitted); see also *Smith*, 442 U.S. at 744-45 (telephone user did not have expectation of privacy in telephone numbers he dialed because that information was "voluntarily conveyed").

This analogy argument also fails because IP log information is not analogous to dialed telephone number information, just as the *Third Circuit Opinion* rejected the claim that a phone company's cell site location information ("CSLI") was analogous to dialed telephone number information. *Third Circuit Opinion*, 620 F.3d at 317-18 (rejecting analogy of CSLI to dialed phone numbers and distinguishing *Smith* and *Miller*). In both *Miller* and *Smith*, the relevant documents and dialed numbers were directly, visibly and knowingly conveyed to bank tellers and telephone operators or their automated equivalents. See, e.g., *Smith*, 442 U.S. at 744 ("When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that informationThe switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed the calls for the subscriber"). Put simply, the phone customer knew and saw what numbers he was exposing to the phone company; the bank customer knew and saw what documents he was exposing to the bank.

In contrast, the Twitter IP log information at issue are much more like CSLI, which can tracked was stored in. *Karo*, 468 U.S. 720.

reveal private location information protected under *Karo*, and like the prolonged GPS tracking information at issue in *Maynard*, and thus the IP log information is similarly protected. IP log information is passively communicated without any direct action or knowledge of, or visibility to, the user, much like the CSLI that the Third Circuit Opinion recognized may be protected by the Fourth Amendment. See *Third Circuit Opinion*, 620 F.3d at 312-13. Such automatic, passive and largely hidden exposure of IP information to a web-based service provider like Twitter is nothing like the direct, visible conveyance of phone numbers to an operator or bank documents to a teller. An Internet user has no similar knowledge and takes no similar voluntary action regarding the exposure of her IP information when visiting web sites such as Twitter. She does not “dial” or type in her IP address; her web browser does not show her that address or indicate that it is being transmitted; she likely has no knowledge of the address at all. The Internet user’s situation is like that of a cell phone user: when a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed, and there is no indication to the user that making that call will also locate the caller, let alone generate a permanent record of this location. When a cell phone user receives a call, he hasn’t voluntarily exposed anything at all.⁷ *Third Circuit Opinion*, 620 F.3d at 317 (“A cell phone customer has not ‘voluntarily’ shared his location information with a cellular provider in any meaningful way.”). In sum, the IP logs sought here are distinguishable from the information at issue in *Miller and Smith* and directly analogous to the CSLI at issue in the *Third Circuit Opinion*. Therefore, *Karo* and *Kyllo* control the reasonable expectation of privacy analysis here.

In its attempt to forestall this conclusion, the Government implies—without any factual record to rely on—that “in an increasingly tech-savvy world” it should be assumed that all Internet users know that they are exposing their IP address, just as all telephone users know they are exposing dialed numbers. Even if the Government’s sweeping claim were correct—and the

⁷ Nor does the IP address appear in the typical Internet user’s bill, a critical fact in *Smith*. See *Smith*, 442 U.S. at 742 (“All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills.”).

logic of the *Third Circuit Opinion* shows why the Government is wrong—that would not settle the question. Even the *Smith* Court recognized that the question of “knowing exposure” was not dispositive in itself, or else *Smith* would have overruled the Court’s prior holding that telephone users have a reasonable expectation of privacy in their phone calls:

A telephone call simply cannot be made without the use of telephone company property and without payment to the company for the service. The telephone conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment. Yet we have squarely held that the user of even a public telephone is entitled “to assume that the words he utters into the mouthpiece will not be broadcast to the world.”

Smith, 442 U.S. at 746-47 (Stewart, J. dissenting) (quoting *Katz v. United States*, 389 U.S. 347, 352 (1967)).

Considering *Katz*, and rather than mechanically applying a “knowing exposure” rationale, the *Smith* Court also had to consider the *invasiveness* of the surveillance at issue, and reasoned that surveillance of dialed numbers was not meaningfully invasive of privacy:

“Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed—a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.”

Smith, 442 U.S. at 741 (quoting *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 167 (1977)).

IP logs are different. They are intensely revealing even though they do not contain the content of a communication, by virtue of the information they reveal about the interiors of private spaces and one’s movements between those spaces. Such information, which can paint an intimate portrait of movements over an extended period of time, is far different from the telephone numbers in *Smith*. See *Maynard*, 615 F.3d at 559-565 (finding reasonable expectation of privacy against prolonged surveillance of movements despite those movements being individually exposed to the public).

Therefore, even if all Twitter users actually read and understand the privacy policy proffered by the Government (Obj. at 16), a dubious proposition for which the Government can

offer no evidence,⁸ those users still maintain an expectation of privacy in their location as reflected in those logs. The mere fact that Twitter may also access that information is not dispositive, as demonstrated in a recent Sixth Circuit decision regarding Fourth Amendment protection for email. *See United States v. Warshak*, No. 08-3997, ___ F.3d ___, 2010 WL 5071766 (6th Cir. Dec. 14, 2010). Email users understand that their email provider stores copies of their messages, and may be subject to similar terms of service or privacy policies stating that the provider may access that content in the ordinary course of business. Yet the Sixth Circuit had no difficulty concluding that email users nevertheless maintain an expectation of privacy in their emails stored with the provider regardless of the terms of the provider's contract with the user. *Warshak*, 2010 WL 5071766, at *12-13.

In *Warshak*, the Sixth Circuit concluded that "it is manifest that agents of the government cannot compel a commercial ISP [or "Internet Service Provider"] to turn over the contents of an email without triggering the Fourth Amendment," and "[i]t only stands to reason that, if government agents compel an ISP to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search, which necessitates compliance with the warrant requirement absent some exception." 2010 WL 5071766 at *12. The *Third Circuit Opinion* similarly assumed that the Fourth Amendment would require a probable cause warrant to the extent that CSLI sought with a § 2703(d) order would reveal information about the interior of a home that is protected under *Karo* or *Kyllo*. *See Third Circuit Opinion*, 620 F.3d at 312-313; *see also id.* at 320 (Tashima, J., concurring). The same is true here: Government access to the IP logs would violate Parties' expectations of privacy, and therefore constitutes a search or seizure requiring a warrant.

⁸ Studies consistently show that vast numbers of Internet users misunderstand the purpose and meaning of online privacy policies. For example, "47% of U.S. adults who use the internet at home say website privacy policies are easy to understand. However, 66% of those who are confident about their understanding of privacy policies also believe (incorrectly) that sites with a privacy policy won't share data." Joseph Turow, *Americans & Online Privacy, The System is Broken*, Annenberg Public Policy Center (June 2003) at 4, *available at* http://www.annenbergpublicpolicycenter.org/Downloads/Information_And_Society/20030701_America_and_Online_Privacy/20030701_online_privacy_report.pdf.

The Government also cannot rely on a Ninth Circuit holding that Internet “pen register” surveillance that captures the IP addresses connected to by a target’s computer does not implicate the Fourth Amendment.⁹ Obj. at 15-17, citing *United States v. Forrester*, 512 F.3d 500, 510. That case was both wrongly decided and is distinguishable. First, it was wrongly decided because it failed to grapple with the same issue that was dispositive in *The Third Circuit Opinion*—the fact that Internet users, like cell phone users and their CSLI, do not in fact voluntarily or knowingly take any action to disclose information about their IP addresses when they use the Internet. Therefore *Forrester*’s brief and mechanical application of *Smith* to Internet addressing information, without any consideration of this key difference, is not persuasive.

Second, *Forrester*’s logic does not apply here because unlike in that case, where IP addressing information was actually used by a target’s Internet Service Provider to route his communications and therefore was arguably analogous to dialing information, Twitter in this case makes no such use of the IP logs it keeps. In other words, unlike the information at issue in *Forrester*, the IP information held by Twitter was “merely passively conveyed through third party equipment” and not “voluntarily turned over to direct the third party’s servers” as in *Forrester. Id.*, 512 F.3d at 510. Furthermore, the information at issue in *Forrester*—the IP addresses of web sites that a target visited using his home computer, as opposed to the IP logs of the sites that a person visited from multiple IP addresses—did not at all implicate locational privacy as the logs at issue here do. The logs in *Forrester* revealed only where a target was going in cyberspace; the logs here reveal the Parties’ movements in the real world.

In sum, the Twitter IP logs reveal information about Twitter users’ locations in private spaces that is protected under *Karo*, and information about their movement between private

⁹ The other cases cited by the Government are equally unavailing. The mechanical application of *Smith* in *United States v. Christie*, 624 F.3d 558, 573-74 (3d Cir. 2010), is even more glancing than in *Forrester*—lasting only a paragraph—and primarily relies on *Forrester*’s flawed reasoning even though the *Forrester* holding was strictly limited to pen register surveillance. 512 F.3d at 510. Meanwhile, the Fourth Circuit’s decision in *United States v. Bynum*, 604 F.3d 161 (4th Cir. 2010), is wholly off point. It concerns only “basic subscriber” information that was obviously and affirmatively conveyed by the user to his internet and telephone service providers, “i.e., his name, email address, telephone number, and physical address....” Such basic subscriber information is not analogous to a passively exposed IP address that the user may not even be aware of.

spaces that is protected under *Maynard*. Twitter users' expectation of privacy in that information is not mitigated by the fact that Twitter records or has access to that information, as made clear by the *Third Circuit Opinion* and *Warshak*. The Court should exercise its discretion under § 2703(d) to vacate the Order and avoid such serious constitutional questions.

E. The Court should vacate the Order to preserve important First Amendment freedoms.

The Government also seeks to brush aside the Parties' First Amendment concerns by claiming, incorrectly, that the Order "is not conceptually different from a routine subpoena seeking telephone subscriber information and toll records from a telephone company." Obj. at 11. This is wrong. As explained above, the IP logs sought here are not at all analogous to dialed phone numbers because IP addresses are passively communicated without any direct action or knowledge of the user. This fact takes the Order out of the pen register context.

Moreover, the Government's argument misses the point. The only apparent reason why the Parties' records are sought here is because they have spoken publicly about WikiLeaks on Twitter.¹⁰ Thus, the Government is seeking to reign in, or punish, or silence speech and/or association it apparently finds distasteful, or embarrassing, or inconvenient. The Government backhands the free speech and association implications of its fishing expedition by claiming "[n]othing remains to fish for" because the Parties "and their associates have already made their postings available for all the world to see." Obj. at 12. This begs the question of why the Government insists on such secrecy and why it sought a § 2703(d) Order—based on an *ex parte* sealed Application—in the first place. Clearly, the Government is seeking more information than the Parties shared with the world.¹¹

¹⁰ Again, the Government refuses to provide the Parties with its Application for the 2703(d) Order, denying the Parties the opportunity to respond directly to it.

¹¹ The Government claims that it has narrowed the scope of the Twitter Order, but that is of no moment to the analysis here because it continues to insist on disclosure of private IP address information and other records that the Parties do not share freely. Moreover, the Parties understand that the Government's "narrowing" is really just an agreement that Twitter need not produce records that it does not possess or that are overly burdensome to produce. The Government has reserved its right to seek additional information in the future and refused to withdraw any portion of the records requests altogether. *See Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 189 (2000) ("voluntary cessation of a challenged practice does not deprive a federal court of its power to determine the legality of the

Despite its claims to the contrary (Obj. at 12), the Government's Application and the resultant Order threaten both speech and association rights. The Government objects that the Parties "fail to explain how the Order chills their freedom of speech or association" (Obj. at 12), but the Parties' moving papers did just that. Mtn. at 8-10. Regardless, no such showing is even necessary. Courts have long recognized that First Amendment claims raise special concerns and that courts can consider the chilling effect of governmental action even before speech or association is actually affected. Pre-enforcement challenges to government requirements that chill speech or association are commonplace and Courts, including the Supreme Court, have routinely permitted such pre-enforcement challenges. *See, e.g., Virginia v. Am. Booksellers Ass'n, Inc.*, 484 U.S. 383, 392-93 (1988) (permitting pre-enforcement challenge in a First Amendment case); *City of Lakewood v. Plain Dealer Publishing Co.*, 486 U.S. 750, 755-57 (1988) (one subject to a potentially unconstitutional licensing law "may challenge it facially without the necessity of first applying for, and being denied, a license").

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

The Government urges the Court to dismiss the Parties' First Amendment concerns out of hand, but Fourth Circuit authority does not permit such cursory review. The Government argues that its desire to uncover private details underlying the Parties' speech on Twitter is akin to a grand jury subpoena related to sexually explicit films. *See* Obj. at 11 (relying on *In re: Grand Jury 87-3 Subpoena Duces Tecum*, 955 F.2d 229 (4th Cir. 1992)). It is not. Much of the Parties' speech that is implicated by the Order here involves political speech—speech that is at the core practice.") (internal quotation omitted).

of the First Amendment and cannot be burdened or restrained absent extraordinary circumstances. *Brandenburg v. Ohio*, 395 U.S. 444, 447-48 (1969). Indeed, as detailed in the Parties opening brief, the Parties have used Twitter regularly to discuss political matters, their views on world events and political developments, and a wide variety of other matters of public concern. See Mtn. at 3-4. The Fourth Circuit case the Government relies on explicitly did not resolve “the ‘First Amendment versus Grand Jury’ dilemma” as the Government implies, see *In re: Grand Jury 87-3*, 955 F.2d at 234, and the Court should decline the Government’s request to do so here.

Moreover, even if this matter is analyzed under the case-by-case balancing test the Government urges, the Government has not shown that its “need for the documents” outweighs “the possible constitutional infringement.” *In re: Grand Jury 87-3*, 955 F.2d at 234. The Fourth Circuit has cautioned that “we are not prepared to rubberstamp every subpoena of business records of a commercial enterprise that distributes material in a presumptively protected medium.” *Id.* Indeed, “[s]uch an unchecked subpoena power would allow any prosecutor to target the affairs of a business with whose expressive activities the prosecutor disagrees or when that prosecutor senses the prospect of political profit in so targeting.” *Id.* This Court, therefore, should scrutinize the Government’s Application and reconsider its Order “with special sensitivity” to the Parties’ First Amendment concerns.

The Fourth Circuit’s concerns about protecting First Amendment freedoms in the *Grand Jury 87-3* matter are nothing new. In an earlier related case, the Court reversed the district court and quashed a subpoena seeking corporate records related to distribution of possibly obscene films. *In re Grand Jury Subpoena: SDT*, 829 F.2d 1291 (4th Cir. 1987). In so doing, it emphasized that beyond the necessary threshold relevance showing, the “critical inquiry” for a district court considering a subpoena that implicates First Amendment rights “is whether there is too much indefiniteness or breadth in the things required to be produced by the subpoena.” *Id.* at 1298. The district court failed to make this inquiry and got the balance wrong. As the Fourth Circuit explained, “[t]he district court showed no sensitivity to the need for [a constitutional] balancing and ordered enforcement of the subpoena on a rationale that we find chilling.” *Id.*

Here, the Order is clearly overbroad, as it seeks information about all of the Parties' speech on Twitter, regardless of any connection to the Government's investigation. The Court should critically examine the Government's Application with special sensitivity to the First Amendment concerns it raises and vacate the Order because it is constitutionally overbroad.

F. The Court should vacate the Order as to Ms. Jonsdottir due to International Comity.

The Government does not dispute that its request for information about Ms. Jonsdottir would not be allowed under Iceland's Constitution, a point raised both by the letter from Iceland's Acting Permanent Secretary of State and the Decision by the Inter-Parliamentary Union. Sears Decl. Exhs. 5 and 6. The Government also does not dispute that, because this information would be unavailable to it under Icelandic law, the only reason it can seek this information at all is because Ms. Jonsdottir chose to use an American-based service, Twitter.com, for her speech activities.

The Government raises a red herring in response to the special concerns arising from its demand for information about a member of the Icelandic Parliament, arguing that Ms. Jonsdottir cannot avail herself of the protections of the Speech or Debate Clause of the U.S. Constitution. This is, of course, true. It is also beside the point. The concern here is that allowing the Government to obtain information about a member of the Icelandic Parliament despite the Icelandic constitutional and statutory prohibitions shows a lack of reciprocal goodwill to the nation of Iceland and sets a troubling precedent. Specifically, this incident could be used to subject U.S. members of Congress to demands from foreign government investigators for information about their speech-related activities merely because they used a communications service that was subject to the jurisdiction of that foreign government.¹²

Thus, the concern here sounds in international comity, which is defined by the Supreme

¹² The precedent set here would be troubling in another way as well. U.S. companies seeking to compete in the global marketplace will be disadvantaged if mere use of their services, even from a foreign location, subjects their international customers to the risk of U.S. government investigations due solely to the fact that their records and data are stored here.

Court as “the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens or of other persons who are under the protection of its laws.” *Hilton v. Guyot*, 159 U.S. 113, 164 (1895). The Fourth Circuit has noted that “at base comity involves the recognition that there are circumstances in which the application of foreign law may be more appropriate than the application of our own law.” *In re French*, 440 F.3d 145, 152-53 (4th Cir. 2006). As Justice Blackmun observed, “Comity is not just a vague political concern favoring international cooperation when it is in our interest to do so. Rather it is a principle under which judicial decisions reflect the systemic value of reciprocal tolerance and goodwill.” *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court*, 482 U.S. 522, 555 (1987) (Blackmun, J., concurring in part and dissenting in part) (comity allowed case-by-case consideration of whether the Hague Convention applies to a discovery request aimed at a foreign litigant).

Here, where the Government’s request for information about Ms. Jonsdottir would not be allowed in Iceland under its Constitution and laws, the Court has the discretion to deny the request based upon the values of “reciprocal tolerance and goodwill” underlying international comity.

III. CONCLUSION

For the foregoing reasons, and those discussed in the Parties’ moving papers, the Court should vacate the December 14, 2010 Order.

Dated: February 10, 2011

By: _____


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

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

Attorneys for JACOB APPELBAUM

Dated: February 10, 2011

By:  with permission for:

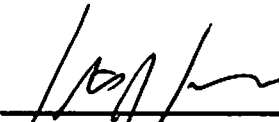
Nina J. Ginsberg, VSB No. 19472
DIMUROGINSBERG, P.C.
908 King Street, Suite 200
Alexandria, VA 22314
Phone: 703-684-4333
Fax: 703-548-3181
Email: nginsberg@dimuro.com

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

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

Attorneys for ROP GONGGRIJP

Dated: February 10, 2011

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

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

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

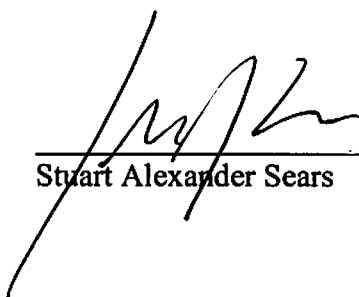
Aden J. Fine (admitted *pro hac vice*)
Benjamin Siracusa-Hillman (admitted *pro hac vice*)
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Telephone: (212) 549-2500
Facsimile: (212) 549-2651
Email: afine@aclu.org
Email: bsiracusahillman@aclu.org

Attorneys for BIRGITTA JONSDOTTIR

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing motion was sent via e-mail this 10th day of February, 2011, to:

Andrew Peterson, Esq.
John S. Davis, Esq.
Assistant United States Attorney
600 East Main Street
Suite 1800
Richmond, VA 23219-2447
Ph: 804-819-7431
Andy.Peterson@usdoj.gov
John.S.Davis2@usdoj.gov



Stuart Alexander Sears