THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

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

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

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

Factual & Procedural Background

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

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

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

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

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

Argument

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

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

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

I. The Order Was Properly Issued.

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

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

(1) endangering the life or physical safety of an individual;

(2) flight from prosecution;

(3) destruction of or tampering with evidence;

(4) intimidation of potential witnesses; or

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

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

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

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

B. The Order Is Constitutional.

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

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

records under 18 U.S.C. § 2703(d), like the Order here.[2] Instead, § 2703(d) provides remedies only for service providers, and only then if "the records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider." 18 U.S.C. § 2703(d). The Stored Communications Act provides that the "remedies and sanctions described in [the Act] are the only judicial remedies and sanctions for nonconstitutional violations of [the Act]." Thus, Congress did not provide wide ranging remedies that would allow subscribers, such as [redacted], to challenge non-content orders, such as the Order here.[3]

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Conclusion

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

Respectfully Submitted,

[redacted]
United States Attorney

By: [redacted]
Assistant United States Attorney

CERTIFICATE OF SERVICE

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

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

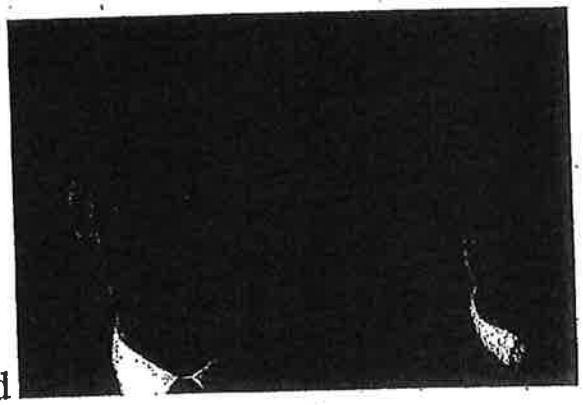
Assistant United States Attorney

GOVERNMENT EXHIBIT 1

Fri, 07 Jan 2011 17:08:00 ET

DOJ subpoenas Twitter records of several [redacted] volunteers

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



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

- Blog:
  - Glenn Greenwald
- Topics:
  - WikiLeaks

(updated below - Update II - Update III)

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

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

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

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

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

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

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

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

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

UPDATE III: [redacted] Interior Minister, Ögmundur Jónasson, described the DOJ's efforts to obtain the Twitter information of a [redacted] as "grave and odd." While suggesting some criticisms of [redacted], he added: "if we manage to make government transparent and give all of us **some insight into what is happening in countries involved in warfare it can only be for the good.**" The DOJ's investigation of a [redacted]t -- as part of an effort to intimidate anyone supporting [redacted] and to criminalize journalism that exposes what the U.S. Government does -- is one of the most extreme acts yet in the Obama administration's always-escalating war on whistleblowers, and shows how just excessive and paranoid the administration is when it comes to transparency: all this from a President who ran on a vow to have the "most transparent administration in history" and to "Protect Whistleblowers."

U.S. Department of Justice

United States Attorney

Eastern District of Virginia

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

FACSIMILE TRANSMISSION COVER PAGE

DATE: 12/14/10

TO: Twitter Attn: Trust & Safety

PHONE:

TO FAX NO.: (415) 222-9958

SENDER: [redacted], Assistant to [redacted]

SENDER'S PHONE NO.: 703 [redacted]

SENDER'S FAX NO.: 703 [redacted]

NUMBER OF PAGES: 4 *Not Including Cover Page*

Level of Transmitted Information:

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

CONTENTS:

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

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

ORDER

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

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

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

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

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

[redacted]
United States Magistrate Judge

12/14/10
Date

ATRUE COPY
CLERK, U.S. DISTRICT COURT
[redacted]
BY DEPUTY CLERK

ATTACHMENT A

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

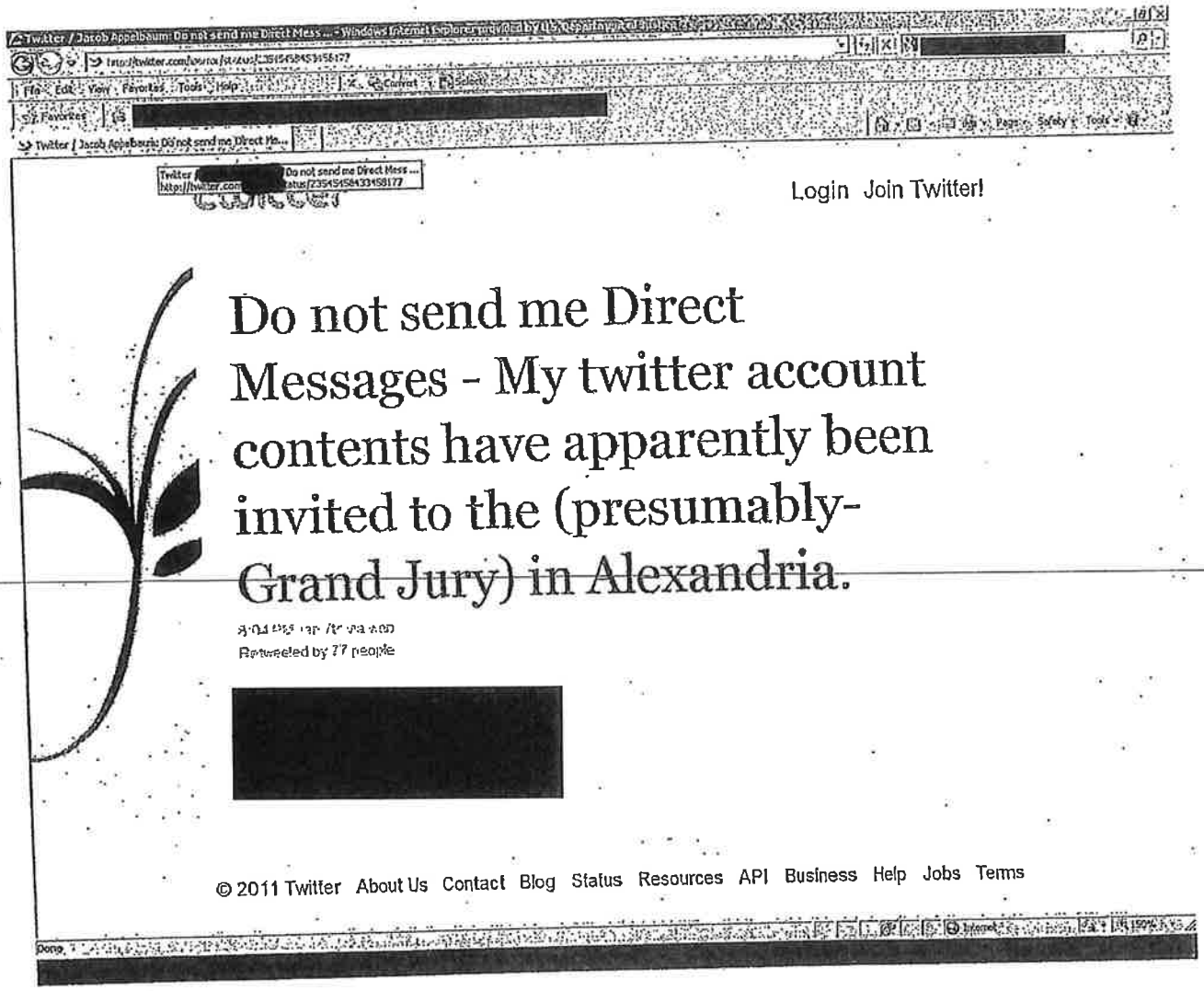
A. The following customer or subscriber account information for each account registered to or associated with [redacted] for the time period November 1, 2009 to present:

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

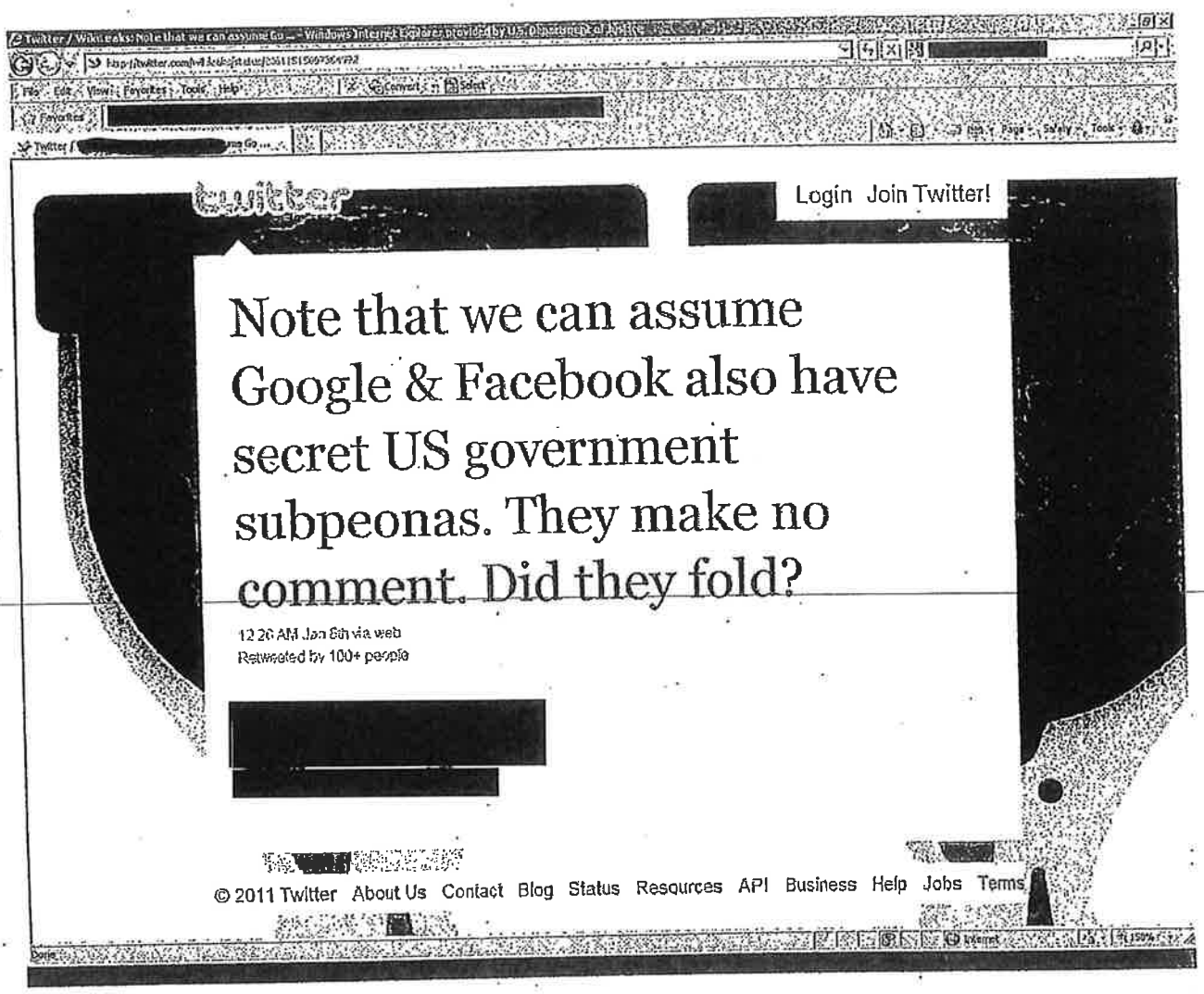
B. All records and other information relating to the account(s) and time period in Part A, including:

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

GOVERNMENT EXHIBIT 2


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

GOVERNMENT EXHIBIT 3


Twitter / Wikileaks: Note that we can assume Go... - Windows Internet Explorer provided by U.S. Department of Justice
Login Join Twitter!
Note that we can assume Google & Facebook also have secret US government subpeonas. They make no comment. Did they fold?
12:26 AM Jan 5th via web
Retweeted by 100+ people
© 2011 Twitter About Us Contact Blog Status Resources API Business Help Jobs Terms

GOVERNMENT EXHIBIT 4

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

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

On the Twitter court order

Dear journalists,

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

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

What happened?

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

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

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

So what does Twitter have on me?

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

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

Why did this happen?

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

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

So what am I going to do now?

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

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

US DOJ wants my twitter account info

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

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

GOVERNMENT EXHIBIT 5

Twitter subpoena

From Wikipedia, the free encyclopedia

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

Contents

Chronology

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

Subpoena issued with accompanying gag order

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

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

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

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

Appeal and publication of the subpoena

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

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

Users' opposition to the subpoena

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

Subsequent reactions

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

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

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

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

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

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

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

See also

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

References

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

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

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

11 January 2011. http://www.webcitation.org/5vfcfKKYI. Retrieved 12 January 2011.
21. ^ Sherington, Greg (11 January 2011). "US Subpoena of Iceland Twitter Accounts" (http://sydney.edu.au/news/law/436.html?newscategoryid=67&newsstoryid=6261) . Sydney Law School. http://sydney.edu.au/news/law/436.html?newscategoryid=67&newsstoryid=6261. Retrieved 13 January 2011.
22. ^ "Anonymous urges global protests" (http://www.bbc.co.uk/news/technology-12191486) . BBC. http://www.bbc.co.uk/news/technology-12191486. Retrieved 17 January 2011.
23. ^ "ALDE Calls on Commission to clarify issue of US Government [redacted] subpoenas" (http://www.alde.eu/press/press-and-release-news/press-release/article/alde-calls-on-commission-to-clarify-issue-of-us-government-wikileaks-subpoenas-36732/) . Alliance of Liberals and Democrats for Europe. http://www.alde.eu/press/press-and-release-news/press-release/article/alde-calls-on-commission-to-clarify-issue-of-us-government-[redacted]-subpoenas-36732/. Retrieved 17 January 2011.
24. ^ "Social Media and Law Enforcement: Who Gets What Data and When?" (http://www.eff.org/deeplinks/2011/01/social-media-and-law-enforcement-who-gets-what) . Electronic Frontier Foundation. http://www.eff.org/deeplinks/2011/01/social-media-and-law-enforcement-who-gets-what. Retrieved 22 January 2011.

External links

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

GOVERNMENT EXHIBIT 6

[redacted]

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

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

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

FILED

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

2011 JAN 18 P 12:58

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

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

NOTICE OF HEARING

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

DATED this 18th day of January, 2011.

Respectfully submitted,

By _____

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

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

Attorneys for Google Inc.

CERTIFICATE OF SERVICE

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

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

Attorneys for the United States

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

Attorneys for Google Inc.