Washington Journal of Law, Technology & Arts

Volume 8 | Issue 4 Article 2

2-1-2013

What Your Tweet Doesn't Say: Twitter, Non-Content Data, and the Stored Communications Act

Daniel Shickich

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 8, ISSUE 4 WINTER 2013

WHAT YOUR TWEET DOESN'T SAY: TWITTER, NON-CONTENT DATA, AND THE STORED COMMUNICATIONS ACT

Daniel Shickich[*]

Cite as: 8 WASH. J.L. TECH. & ARTS 457 (2013)
http://digital.law.washington.edu/dspace-law/handle/1773.1/1226

ABSTRACT

A federal district court in Virginia recently held that Twitter users have no privacy rights regarding non-content information associated with their use of Twitter. The court thus affirmed that the government may obtain Twitter users' Internet Protocol (IP) addresses without notice to the users. The users in this case were alleged to be members of WikiLeaks. The government obtained an order of production in connection with grand jury proceedings, compelling Twitter to turn over IP address data to the government. After Twitter motioned to have the order unsealed, the alleged WikiLeaks members unsuccessfully attempted to intervene to quash the order of production. The district court found that the users lacked standing to challenge the order under the Stored Communications Act (SCA) because Twitter's terms of use negated any expectations of privacy and the nature of IP address data itself requires that users convey IP addresses and associated information in order to use the Internet. This Article examines the court's decision and analysis under the SCA and Fourth Amendment jurisprudence, and discusses the impact of expanded warrantless disclosures of non-content electronic records.

---

[*] Daniel Shickich, University of Washington School of Law, Class of 2013. Thank you to Professor Jane Winn, University of Washington School of Law, Peter Winn, United States Department of Justice, and student editor Bryan Russell for their help with this Article.

TABLE OF CONTENTS

INTRODUCTION

More Americans are using social media to communicate than ever before, and using a wide array of devices, from personal computers to cellular phones, to do so. Online social networking sites—such as Twitter, Facebook, MySpace, LinkedIn, and FourSquare—are ubiquitous. For example, Twitter use is increasingly prevalent among nearly every demographic group in the United States. A 2011 Pew Research survey found that 13 percent of adults that use the Internet use Twitter.[1] The survey also found pronounced growth in the number of non-white Twitter users, as well as significant growth in the number of Twitter users age 25-44.[2] Such trends appear consistent with the growth of online social media in general; as of 2011, 65 percent of online adults used social networking sites such as MySpace, Facebook, or

[1] Aaron Smith, *Twitter Update 2011*, PEW RESEARCH CENTER, June 1, 2011, http://www.pewresearch.org/pubs/2007/twitter-users-cell-phone-2011-demographics.

[2] *Id.*

LinkedIn.[3] Considering that in February 2005, only 8 percent of adult Internet users used social networking sites, the pace of growth for online social networking site is "staggering."[4]

Unlike email messages and other predecessors to modern social media, communications through online social media are often publicly available—at least to other members of the social network. The public nature of many online social networks reduces or eliminates any expectation of privacy as to the content of the messages themselves. Government entities pursuing evidence of criminal activity through the records of online social networking sites do not always seek the actual content of the communications, but rather seek the non-content data—including the identity and location of the user. As a result, questions regarding privacy and government access to electronic non-content records arise relating to the Stored Communications Act (SCA), 18 U.S.C. § 2701 *et seq.* (2010). Because non-content data,[5] such as an Internet Protocol (IP) address, is necessary for communication via the Internet, many social networking companies routinely retain such information.

A federal district court in Virginia recently held that the federal government may obtain Twitter users' Internet Protocol (IP) addresses without notice to the users. This decision represents a

---

[3] Mary Madden & Kathryn Zickuhr, 65*% of Online Adults Use Social Networking Sites*, PEW RESEARCH CENTER, Aug. 26, 2011, http://pewinternet.org/Reports/2011/Social-Networking-Sites/Overview.aspx.

[4] *Id*.

[5] Non-content information has been described as "the envelope information needed to deliver a communication from one location to another." WAYNE R. LAFAVE, JEROLD H. ISRAEL, NANCY J. KING & ORIN S. KERR, 2 CRIM. PROC. § 4.4(D) (3d ed. 2011). Under the SCA, non-content information includes:

> (A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account number)."

18 U.S.C. § 2703(c)(2) (2010); *see also* WAYNE R. LAFAVE, JEROLD H. ISRAEL, NANCY J. KING & ORIN S. KERR, 2 CRIM. PROC. § 4.8(C) (3d ed. 2011).

natural application of existing Fourth Amendment jurisprudence applying the SCA. Further, the decision gives notice to both users and operators of social networks that there is no expectation of privacy for IP address data transmitted over the Internet—even when the data is transmitted from a personal computer located in a private space.

This Article examines the federal district court's decision and analysis under SCA and Fourth Amendment jurisprudence. Then, this Article discusses the impact of expanded warrantless disclosures of non-content electronic records on online social networking sites and users. The Article concludes by noting that the nature of online communication itself requires that non-content data be disclosed between machines, meaning that under the SCA, certain data required for using the Internet is inherently non-private.

I. TWITTER AND NON-CONTENT DATA

A. Twitter

Twitter is an online social media network that allows users to post short messages to one another or to the public. The company's website states, "Twitter is a real-time information network that connects [users] to the latest stories, ideas, opinions and news about what [users] find interesting."[6] Twitter users communicate using "tweets." Each tweet is up to 140 characters long; users can share photos, videos and conversations directly in tweets.[7] Twitter allows users to post tweets and read the tweets of other users via computers and other mobile devices that connect to the Internet. Users can monitor, or "follow," other users' tweets, and can permit or forbid access to their own tweets. In addition to posting their own tweets, users may send messages to a single user ("direct messages") or repost other users' tweets ("retweet"). Each Twitter user has a unique username, which is associated with that user's

---

[6] *About Twitter*, TWITTER.COM, http://twitter.com/about (last visited Jan. 3, 2013).

[7] *Id.*

tweets, direct messages, and retweets.[8]

Twitter requires that users agree to a "clickwrap"[9] agreement that includes agreeing to Twitter's Terms of Service and Privacy Policy as a condition of creating a Twitter account.[10] The Privacy Policy includes a number of key terms and conditions that relate to retention of user data. For example, the Privacy Policy as of May 17, 2012 explained that, "We may preserve or disclose your information if we believe that it is reasonably necessary to comply with a law, regulation or legal request; to protect the safety of any person; to address fraud, security or technical issues; or to protect Twitter's rights or property."[11] Additionally, the Policy states that:

> Our servers automatically record information ("Log Data") created by your use of the Services. Log Data may include information such as your IP address, browser type, operating system, the referring web page, pages visited, location, your mobile carrier, device and application IDs, search terms, and cookie information. We receive Log Data when you interact with our Services, for example, when you visit our websites, sign into our Services, interact with our email notifications, use your Twitter account to authenticate to a third-party website or application, or visit a third-party website that includes a Twitter button or widget. Twitter uses Log Data to provide our Services and to measure, customize, and improve them. If not

---

[8] *In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. §2703(d), 830 F. Supp. 2d 114, 118 (E.D. Va. Nov. 10, 2011) (internal footnotes omitted); *see also* Rafe Needleman, *Newbie's guide to Twitter*, CNET, March 15, 2007, http://news.cnet.com/newbies-guide-to-twitter/.

[9] In computer software, hardware, and Internet transactions terms and conditions are often contained in a clickwrap agreement—terms and conditions that appear on the computer screen when the user attempts to install the software or use the website and require that a consumer agree to the license terms before being allowed to purchase or use the product or website. 15B AM. JUR. 2D *Computers and the Internet* § 105 (2012).

[10] *In re Application*, 830 F. Supp. 2d at 118.

[11] *Twitter Privacy Policy*, TWITTER.COM, May 17, 2012, http://twitter.com/privacy.

> already done earlier, for example, as provided below for Widget Data, we will either delete Log Data or remove any common account identifiers, such as your username, full IP address, or email address, after 18 months.[12]

Users must acknowledge and agree to this Privacy Policy as a condition of using Twitter.

B. 18 U.S.C. § 2703: Content or Non-Content Under the SCA

Enacted as Title II of the Electronic Communications Privacy Act of 1986,[13] the SCA largely governs the methods and requirements for government access to electronically stored communications and the data related to those communications. The SCA draws an important distinction between content and non-content information in Section 2703. In addition to establishing the procedures by which the government may obtain access to electronic communications and information, the section distinguishes between "contents" and non-content "records."[14]

The SCA distinguishes between content substance and form. When the government seeks "information concerning the substance, purport, or meaning of that communication" (in other words, content), paragraphs (a) and (b) apply.[15] If, on the other hand, the government seeks non-content records, paragraph (c) controls.[16] Section 2703, paragraph (c)(2) lists the type of non-content data subject to disclosure, including the subscriber or

---

[12] *Id.*

[13] Pub.L. No. 99–508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2701–2711 (2010)). The Electronic Privacy Act of 1986 was enacted in part to extend enhanced privacy protections to developing forms of telecommunications and computer technology, including cellular phones, pagers, and email. *See* S. Rep. No. 99–541 at 4 (1986), reprinted at 1986 U.S.C.C.A.N. 3555, 3559; *see generally* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208,1209-13 (2008).

[14] 18 U.S.C. § 2703 (2010); *see also* Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

[15] 18 U.S.C. §§ 2510(8), 2703(a)-(b), 2711(1) (2010).

[16] 18 U.S.C. § 2703(c) (2010).

customer name, address, telephone connection records or records of session times and durations, length and type of service used, telephone number or temporarily assigned network address, and method of payment.[17] "Although the line between [content and non-content] occasionally blurs, in most cases the line is clear: it is the line between a message that a person wants to communicate and information about when and how he does so."[18] Under the SCA, data associated with a subscriber or customer is non-content, whereas information contained in the communication itself is content.

According to the SCA, a court order issued under 18 U.S.C. § 2703(c) for non-content records "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."[19] This court order is "something like a mix between a subpoena and a search warrant. . . . If the judge finds that the factual showing has been made, the judge signs the order. The order is then served like an ordinary subpoena . . ."[20] The order does not require notification to the customer or subscriber when the government requests non-content records under paragraph (c).[21]

II. *IN RE APPLICATION OF THE U.S. FOR AN ORDER PURSUANT TO 18 U.S.C. §2703(D)*[22]

In a memorandum opinion issued on November 10, 2011, a federal district court judge in Virginia addressed the limitations of

---

[17] 18 U.S.C. § 2703(c)(2) (2010).

[18] Kerr, *supra* note 13, 1228.

[19] 18 U.S.C. § 2703(d) (2010).

[20] Kerr, *supra* note 13, 1219.

[21] 18 U.S.C. § 2703(c)(3) (2010). The requirements for accessing content information are far more complex and vary in part based on whether the content has been in "electronic storage" more or less than 180 days. *See* WAYNE R. LAFAVE, JEROLD H. ISRAEL, NANCY J. KING & ORIN S. KERR, 2 CRIM. PROC. § 4.8(D) (3d ed. 2011).

[22] 830 F. Supp. 2d 114 (E.D. Va. Nov. 10, 2011).

the Fourth Amendment right to privacy with regard to Internet communications. The opinion affirms a United States magistrate judge's rulings regarding an order of production issued under the SCA that allowed the government to obtain non-content records regarding Twitter users without a warrant. Petitioners, three alleged members of the WikiLeaks organization[23] facing potential criminal charges over public disclosure of classified information about the Iraq and Afghanistan wars, moved to quash the order, unseal the application seeking the order, and publicly docket other related information on a variety of grounds, including a constitutional claim based on the Fourth Amendment right to privacy. In denying petitioners' motions, the judge noted that gaining online access requires all Internet users to transmit IP address information associated with their personal computing devices out of private home spaces and onto online routers that then convey traffic to specific websites. Combined with Twitter's privacy policy, which resulted in application of the Fourth Amendment's third-party doctrine, the nature of Internet data transmission led the judge to conclude that Twitter users have no expectation of privacy regarding the numerical IP addresses that identify their computers, cellular phones, or other mobile devices that connect to the Internet when using Twitter.

A. Factual Context

As part of an ongoing criminal investigation into alleged leaks of classified United States military documents related to the Iraq and Afghanistan wars, the federal government sought a court order based on 18 U.S.C. § 2703(d) instructing Twitter, Inc. to turn over information pertaining to three individuals under grand jury investigation.[24] The government alleged that the three

[23] WikiLeaks is an international, online, self-described "not-for-profit media organisation" that seeks to publish original source material and news stories based on information leaked from a variety of anonymous sources. *About*, WIKILEAKS.COM, http://wikileaks.org/About.html (last visited Jan. 3, 2013).

[24] In re *Application*, 830 F. Supp. 2d at 117; Scott Shane & John F. Burns, *U.S. Subpoenas Twitter Over WikiLeaks Supporters*, N.Y. TIMES, Jan. 8, 2011, http://www.nytimes.com/2011/01/09/world/09wiki.html?pagewanted=all&_r=0.

individuals—Jacob Appelbaum, a resident and citizen of the United States and a computer security expert, Rop Gonggrijp, a Dutch citizen and a computer security expert, and Birgitta Jonsdottir, a citizen and resident of Iceland, and a member of the Icelandic parliament—acted as members of the Wikileaks organization and performed criminal acts related to the release of classified U.S. government documents.[25] The three were alleged to be subscribers and users of Twitter, and used the Internet to communicate with the Twitter social networking site.[26]

B. Procedural Posture

Upon *ex parte* application by the government, Magistrate Judge Theresa Carroll Buchanan issued an order instructing Twitter to produce specific electronic records to the government.[27] Twitter responded with a motion to unseal the order. On January 5, 2011, based on Twitter's motion and the government's consent, the magistrate judge unsealed the order, finding that it was in the best interest of the investigation.[28] The magistrate judge also authorized Twitter to disclose the order to Appelbaum, Gonggrijp, and Jonsdottir.[29]

In response, the three individuals filed a motion to vacate the order, and a motion to unseal certain other court records pertaining to the order and publicly docket all orders issued under 18 U.S.C. § 2703.[30] The individuals based their motions on a variety of grounds, including a constitutional claim based on the Fourth Amendment right to privacy.[31]

After briefing from both parties, Magistrate Judge Buchanan issued an order and memorandum opinion denying the motion to vacate, granting in part the motion to unseal, and keeping under

---

[25] *In re Application*, 830 F. Supp. 2d at 117.
[26] *Id.*
[27] *Id.* at 121.
[28] *Id.* at 122.
[29] *Id.*
[30] *Id.*
[31] *Id.* at 127.

advisement the issue of public docketing.[32] In her memorandum opinion, Magistrate Judge Buchanan found that the individuals lacked standing to challenge the order, that issuance of the order was proper under the SCA, and that issuance of the order did not violate the Fourth Amendment.[33] Then, on June 1, 2011, Magistrate Judge Buchanan issued an order and memorandum opinion denying the request for public docketing.[34] Appelbaum, Gonggrijp, and Jonsdottir filed objections to both orders.[35]

C. Building on Prior Precedent

On November 10, 2011, Federal District Court Judge Liam O'Grady affirmed the rulings of Magistrate Judge Buchanan, finding that the individuals lacked statutory standing.[36] The judge further found that the order of production issued under the SCA that allowed the government to obtain non-content Twitter information was valid, did not require a warrant, and did not violate any Fourth Amendment right to privacy.[37]

In denying petitioners' motions, Judge O'Grady noted that gaining online access requires all Internet users to transmit IP address information associated with their personal computing devices out of private home spaces and onto online routers that then convey traffic to specific websites.[38] Combined with Twitter's privacy policy, which resulted in application of the Fourth Amendment's third-party doctrine, the nature of Internet data transmission led the judge to conclude that Twitter users have no expectation of privacy regarding the numerical IP addresses that identify their computers, cellular phones or other mobile devices that connect to the Internet when using Twitter.[39]

The court first addressed locational privacy issues raised by the

---

[32] *Id.* at 122.
[33] *Id.* at 127.
[34] *Id.* at 122.
[35] *Id.*
[36] *Id.* at 128-29.
[37] *Id.* at 129-30, 138.
[38] *Id.* at 135.
[39] *Id.* at 138.

possible use of non-content data. The court distinguished *United States v. Karo*,[40] noting that the case at bar did not involve surveillance of something that had been withdrawn from view, but rather something that was transmitted from a private space into a public space, and that Twitter, not the government, recorded the information.[41] That such information could be used to pinpoint the location of the user did not worry the court, as "[t]he Fourth Circuit has explicitly approved the collection of non-IP subscriber information" to pinpoint the location of a party.[42] In essence, the court distinguished the facts of this case from those of *Karo*, focusing on the entity making the transmission and the entity recording the data. In addition, the court explained that, assuming *arguendo* that the government was able to track user movements based upon IP address data, "IP addresses are no more revealing about the contents of communication than are phone numbers."[43] Just as the government "may be able to make educated guesses about what was said, simply based on non-content information about the parties involved in the communication" using telephone numbers, so too may the government perform similar guesswork with IP addresses.[44]

The court then examined the impact of the third-party doctrine on the privacy claim. The court noted the history of the third-party doctrine, looking to *United States v. Miller*,[45] and *Smith v. Maryland*.[46] The court explained:

> Like the defendant in *Smith* [relied on the phone company to connect calls], Petitioners relied on Internet technology to access Twitter, indicating an intention to relinquish control of whatever information would be necessary to complete their communication. They knew that their communications with Twitter would be transmitted

---

[40] 468 U.S. 705 (1984).
[41] *In re Application*, 830 F. Supp. 2d at 131-33.
[42] *Id.* at 133 (citing U.S. v. Bynum, 604 F.3d 161, 164 n.2 (2010)).
[43] *Id.* at 138.
[44] *Id.*
[45] 425 U.S. 435 (1976).
[46] 442 U.S. 735 (1979).

> out of private spaces and onto the Internet for routing to Twitter.[47]

Analogizing the defendant's voluntary disclosure of information to the phone company when dialing a phone from within his home in *Smith* to the act of the petitioners in the case at bar in disclosing their IP addresses to Twitter, the court concluded that "[b]oth phone numbers and IP addresses must be revealed to intermediaries as a practical necessity of completing communications over their respective networks."[48]

The court pointed to two prior cases to support its conclusion that IP addresses are analogous to telephone numbers. In *U.S. v. Christie*, the defendant was convicted of possession of thousands of images of child pornography and of various child-pornography-related offenses.[49] The defendant appealed, based in part on an argument that the government's acquisition of his IP address violated his Fourth Amendment rights and thus evidence gathered related to his activity on a child pornography website should have been suppressed.[50] The Third Circuit rejected this argument, analogizing an IP address to other subscriber information and holding that "no reasonable expectation of privacy exists in an IP address."[51] Likewise, in *United States v. Forrester*, a defendant convicted of conspiracy to manufacture ecstasy and various other offenses related to the operation of a large ecstasy-manufacturing laboratory challenged the validity of a government computer surveillance program that enabled the government to learn, among other things, the IP addresses of the websites that he visited.[52] Comparing the gathering of IP address data with the use of a pen register in *Smith*,[53] the Ninth Circuit concluded that the government's actions were not a search within Fourth Amendment purposes.[54]

---

[47] *In re Application*, 830 F. Supp. 2d at 135.
[48] *Id.*
[49] 624 F.3d 558, 562 (3d Cir. 2010).
[50] *Id.* at 567.
[51] *Id.* at 574.
[52] 512 F.3d 500, 504 (9th Cir. 2007).
[53] 442 U.S. 735 (1979).
[54] *Forrester*, 512 F.3d at 510.

The court also distinguished the facts of the Twitter case from those of two other situations that courts have faced. First, the court noted that the petitioners reliance on *United States v. Warshak*[55] was misplaced because *Warshak* dealt with an order seeking emails—in other words, content.[56] In contrast, the government sought only non-content records in the case at bar.[57] Similarly, the Court concluded that *United States v. Heckenkamp*[58] was "inapposite because the intrusion at issue [in *Heckenkamp*] was a remote search of the defendant's computer, which included running commands and examining files stored on the defendant's personal computer."[59] Whereas "[p]ersonal computers are ordinarily treated like closed containers under the Fourth Amendment," the non-content data the users transmitted to Twitter moved from a private space into a public space.[60]

Thus, relying in large part on previous decisions, the Court determined Twitter users lack a reasonable expectation of privacy in the IP data transmitted as part of their communication with the website.

III. IMPACT ON ONLINE SOCIAL NETWORKING SITES AND USERS

A. Non-Content Data is Not Private or Protected

Application of the SCA to social networking sites appears to limit any privacy interests that end users have in information conveyed to the social media service providers, at least in non-content information. Under this court's analysis, it does not appear that the Fourth Amendment would ever protect non-content information contained in or associated with IP addresses. As the Court states, "[The Petitioners] also implicitly consented to disclosure of their IP address information to Twitter as a practical

---

[55] 631 F.3d 266 (6th Cir. 2010).
[56] *In re Application*, 830 F. Supp. 2d at 137.
[57] *Id.*
[58] 482 F.3d 1142 (9th Cir. 2007).
[59] *In re Application*, 830 F. Supp. 2d at 137.
[60] *Id.*

necessity of using Internet technology."[61] IP addresses are necessary to route communications over the Internet. Such a result is consistent with prior decisions and represents a natural expansion of prior precedent.[62] The distinction between content and non-content, as well as the distinction between private and public spaces, remain firm.

The conclusions of others who have considered the application of the SCA to analogous situations also bolster this decision.[63] Because the nature of online communication requires disclosure of IP address data into public space and to a third party, even when transmitted from a personal computer located in a private space, social networking site users and operators should be on notice that no expectation of privacy exists in IP address data transmitted over the Internet.

B. Non-Content Data is Collected and Retained

Social networking sites will continue to track and retain non-content data, including IP address information. For example, both Twitter and Facebook include explicit messages about retaining IP address information in their respective privacy policies.[64] Twitter

---

[61] *Id.* at 139.

[62] *See e.g.*, U.S. v. Christie, 624 F.3d 558, 574 (3d Cir. 2010); U.S. v. Forrester, 512 F.3d 500 (9th Cir. 2007).

[63] *See, e.g.*, Kerr, *supra* note 13, 1210 ("[B]y communicating with their ISPs, Internet users have revealed information to their ISPs and have relinquished their Fourth Amendment rights in that information."); People v. Malcolm Harris, 949 N.Y.S.2d 590 (N.Y. Crim. Ct. June 30, 2012).

[64] According to Twitter, "Our servers automatically record information (Log Data) created by your use of the Services. Log Data may include information such as your IP address, browser type, operating system, the referring web page, pages visited, location, your mobile carrier, device and application IDs, search terms, and cookie information." *Twitter Privacy Policy*, TWITTER.COM, June 23, 2011, http://twitter.com/privacy. Likewise, Facebook states, "We receive data from the computer, mobile phone or other device you use to access Facebook, including when multiple users log in from the same device. This may include your IP address and other information about things like your internet service, location, the type (including identifiers) of browser you use, or the pages you visit." *Data Use Policy*, FACEBOOK.COM, https://www.facebook.com/about/privacy/your-info (last visited Jan. 3, 2013).

informs users that in most cases it will only retain such data for 18 months, after which it will either delete it or remove "common account identifiers" (such as username, full IP address, or email address);[65] Facebook retains data until an account has been deleted.[66]

That private companies are retaining non-content data does not appear to worry the court in this case. After noting that IP addresses are necessary to route communications over the Internet, the court continued:

> The fact that Twitter chose to record IP address information pertaining to [the Twitter users], and the purpose for which it did so, makes no difference. . . . As the Supreme Court stated in *Smith* [*v. Maryland*], the meaning of the Fourth Amendment cannot be dictated by the record-keeping practices of a private corporation. ("We are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here) the pattern of protection would be dictated by billing practices of a private corporation.").[67]

Non-content data is necessarily transmitted and routinely retained. Social networking companies collect and retain non-content data because users necessarily provide it—making it pervasive and uniform. Non-content data helps companies provide more personalized service, and can be used to monetize social networking sites through targeted advertising. And regardless of why non-content data is retained, privacy interests found in the Fourth Amendment or the SCA do not protect it.

---

[65] *Twitter Privacy Policy*, TWITTER.COM, June 23, 2011, http://twitter.com/privacy.

[66] *Data Use Policy*, FACEBOOK.COM, https://www.facebook.com/about/privacy/your-info (last visited Jan. 3, 2013).

[67] *In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. §2703(d), 830 F. Supp. 2d 114, 137-38 (E.D. Va. Nov. 10, 2011) (internal citation omitted).

CONCLUSION

In deciding *In re Application of the U.S. for an Order Pursuant to 18 U.S.C. §2703(d)*, a federal district court in Virginia affirmed that the federal government can legally obtain a Twitter user's IP address and other non-content information associated with the user without first providing notice to the user. This decision represents a natural expansion of existing Fourth Amendment jurisprudence applying the SCA, and gives both users and operators of social networking sites notice that there is no expectation of privacy for IP address data transmitted over the Internet—even when the data is transmitted from a personal computer located in a private space. The nature of online communication itself requires that machines disclose non-content data, meaning that under the SCA, the data required for using the Internet is inherently non-private. Internet users lack a reasonable expectation of privacy in the IP data and other non-content information they transmit as part of their communication with a website.

PRACTICE POINTERS

- All social networking companies should employ "clickwrap" agreements and/or privacy policies that put users on notice regarding the company's retention of non-content data.
- Internet users should be aware that social networking sites (as well as a host of other sites) retain non-content data for a variety of purposes.
- Courts will likely continue to analogize IP address information to telephone numbers when performing any Fourth Amendment analysis.