COMPULSORY PROCESS IN CYBERSPACE: RETHINKING PRIVACY IN THE SOCIAL NETWORKING AGE

ROBERT D. RICHARDS*

INTRODUCTION

When Malcolm Harris crossed the Brooklyn Bridge in October 2011—one among some 700 Occupy Wall Street protesters later charged with disorderly conduct for marching over the expanse—he undoubtedly did not imagine that the incident would place him squarely in the throes of a modern-day privacy battle.[1] Shortly after his arrest for the violation—"the lowest level of-

* John & Ann Curley Professor of First Amendment Studies, Pennsylvania State University; Founding Director of the Pennsylvania Center for the First Amendment, Pennsylvania State University; J.D., American University; Member, State Bar of Pennsylvania. The author thanks Student Fellows Cristina Infanzòn and Samantha Hurley for their research assistance and comments on early drafts of this Article.

1. *See* Emily Jane Goodman, *Manhattan District Attorney Subpoenas Occupy Protester's Twitter Account*, THE NATION, Feb. 15, 2012, http://www.thenation.com/article/166273/manhattan-district-attorney-subpoenas-occupy-protesters-twitter-account.

fense in the New York State Penal Law"[2]—the San Francisco headquarters of Twitter informed the twenty-three-year-old writer that the Manhattan District Attorney's Office had issued a subpoena on the social network to appear "as a witness in a criminal action prosecuted by the People of the State of New York against: Malcolm Harris."[3] More specifically, the subpoena commanded the social network to produce "[a]ny and all user information, including email address, as well as any and all tweets posted for the period of 9/15/2011 – 12/31/2011 for the following twitter account: @destructuremal."[4] The subpoena demanding Harris's user information was not an isolated incident. According to a recent Twitter Transparency Report, the company received 679 government requests for user account information, typically in connection with criminal investigations, in just the first six months of 2012.[5] The company maintains that it has cooperated and produced "some or all information" in 75% of the requests.[6]

The demand for user account information is so great that Twitter has created "Guidelines for Law Enforcement,"[7] which set forth its policy for turning over user information to the government or others. Twitter is not alone in developing such a policy: Other social networks, such as Facebook,[8] LinkedIn,[9] and Dropbox,[10] have similar guidelines.

---

2. *Id.*

3. *Id.*; Subpoena Duces Tecum To Twitter, Inc., People v. Harris, No. 2011NY080152, (N.Y. Crim. Ct. Jan. 26, 2012) (on file with author).

4. Goodman, *supra* note 1.

5. *Twitter Transparency Report*, TWITTER, http://support.twitter.com/groups/33-report-abuse-or-policy-violations/topics/148-policy-information/articles/20170002-twitter-transparency-report (last visited Feb. 2, 2013).

6. *Id.*

7. *Guidelines for Law Enforcement*, TWITTER, https://support.twitter.com/articles/41949 (last visited Feb. 2, 2013) ("[N]on-public information about Twitter users is not released except as lawfully required by appropriate legal process such as a subpoena, court order, or other valid legal process.").

8. *See Law Enforcement & Third-Party Matters*, FACEBOOK, http://www.facebook.com/help/?page=211462112226850 (last visited Feb. 2, 2013) ("We work with law enforcement where appropriate and to the extent required by law to ensure the safety of the people who use Facebook. We may disclose information pursuant to subpoenas, court orders, or other requests (including criminal and civil matters) if we have a good faith belief that the response is required by law.").

9. *See* LINKEDIN, LINKEDIN LAW ENFORCEMENT DATA REQUEST GUIDELINES 2 (2012), http://help.linkedin.com/ci/fattach/get/1568450/0/filename/LinkedIn%20Law%20Enforcement%20Data%20Request%20Guidelines.pdf ("For requests pur-

Harris was not the only "occupier" to face such a subpoena. In Boston, Guido Fawkes "has become a representative of the legal limits of privacy on online social networks."[11] Authorities there used an administrative subpoena—one that requires "only an attorney general's approval"—to find information about Fawkes because he "reportedly posted a link to a website with personal information about Boston police officers, including where they live."[12] Peter Krupp, an attorney for Fawkes, observed that most users of Twitter and other social networks would ''reasonably expect" their speech to be anonymous.[13] Perhaps more disturbing, in late December 2011, a Suffolk Superior Court judge "held a secret hearing over the objections of lawyers from the American Civil Liberties Union (ACLU) of Massachusetts, and then impounded all documents and motions filed in the case."[14] In response, Massachusetts ACLU executive director Carol Rose commented:

> Secret court proceedings, particularly proceedings involving First Amendment issues, are troubling as a matter of both law and democracy. In addition, the manner in which the administrative subpoena in this case was used, and its purported scope, is equally troubling and, in our opinion, well beyond what the Massachusetts statute allows.[15]

Police likewise have been quick to subpoena Twitter for seemingly more urgent matters. In August 2012, New York City police officials obtained a subpoena in an attempt to reveal the identity of a user who threatened to attack a Broadway

---

suant to formal compulsory legal process issued under U.S. law, we will provide records as required by law.").

10. *See Dropbox Law Enforcement Handbook*, DROPBOX, https://dl.dropbox.com/s/77fr4t57t9g8tbo/law_enforcement_handbook.html (last visited Feb. 2, 2013) ("To obtain non-public user information, law enforcement must provide the correct legal documents required for the type of information being sought (e.g., subpoena, order, warrant). To protect our users' rights, we scrutinize all requests to make sure they comply with the law.").

11. Kevin Shalvey, *Twitter Facing a Tricky Dance When Privacy, Subpoenas Clash*, INVESTOR'S BUS. DAILY, Apr. 5, 2012, at A04.

12. *Id.*

13. *Id.*

14. Press Release, ACLU, Court Seals ACLU Challenge to Twitter Subpoena (Dec. 29, 2011), *available at* http://aclum.org/news_12.29.11.

15. *Id.*

theater.[16] Authorities sought a court order after Twitter declined an emergency request by law enforcement.[17] The company reportedly reviewed the user account that concerned the police and concluded, "While we do invoke emergency-disclosure procedures when it appears that a threat is present, specific and immediate, this does not appear to fall under those strict parameters as per our policies."[18] The Manhattan District Attorney's Office subsequently obtained the subpoena, after which police spokesman Paul J. Brown commented, "We felt that a threat involving an identified location in the heart of the theater district merited immediate cooperation."[19]

Shortly thereafter, New York City Police Commissioner Raymond Kelly announced plans to reinforce the NYPD's cyber crackdown by expanding online investigative tactics, making clear that monitoring online activity is now a part of standard police operating procedure.[20] Officials added that "much of the potentially incriminating material they gather can be found on Facebook profiles that are public."[21] In Cincinnati, police have created a Real Time Crime Center, headed by Lieutenant Lisa Thomas, who notes, "You have guys who are bragging about their crimes online."[22] But not all of what the police are looking for is readily available online. Further, law enforcement is dealing with how to balance the proper handling of social media content against privacy concerns. Notably, police are grappling with the limits of the current law that determines what kinds of methods police can use to retrieve per-

16. Wendy Ruderman, *Court Prompts Twitter to Give Data to Police in Threat Case,* N.Y. TIMES, Aug. 8, 2012, at A14 (reporting that the Twitter user had alarmed police with Tweets that said, "I might just shoot up this theater in New York"; "I know they leave their exit doors unlocked"; and "I got 600 people on my hit list and that's gonna be a mass murder for real.").

17. *Id.*

18. *Id.*

19. *Id.*

20. Tom Hays, *NYPD is Watching Facebook to Fight Gang Bloodshed*, ASSOC. PRESS, Oct. 2, 2012, http://bigstory.ap.org/article/nypd-watching-facebook-fight-gang-bloodshed (noting that "police and prosecutors have responded over the past several years by closely monitoring Facebook and other sites for leads and evidence").

21. *Id.*

22. Roger Yu, *Social media's role in police investigations is growing*, USA TODAY, Mar. 19, 2012, at 11B (noting that "[w]ith more netizens flaunting their actions and thoughts in the open, social media has become a mainstay in police work").

sonal data.[23] This problem threatens to become even more exacerbated as the popularity of social networks continues to grow—for example, Facebook contends it "hit a milestone of 1 billion monthly users" in October 2012[24]—even though less than half of all law enforcement agencies have a social media policy for police investigation.[25]

Not all subpoenas designed to extract user information in criminal matters originate from the prosecutorial side of the case. George Zimmerman, the neighborhood watchman charged in the shooting death of a teenager, is using a subpoena against Twitter and Facebook to find evidence suggesting that Trayvon Martin could in fact have been the aggressor on the night that he was killed.[26] Defense attorneys also hope to find out whether "negative rumors about Trayvon's social media comments that have circulated the Internet for months are proven true."[27] Zimmerman's lawyer defended the use of subpoenas, noting, "This is how you defend someone charged with second-degree murder, a charge that presumes ill will and hate."[28] As Nicole Black, co-author of *Social Media for Lawyers: The Next Frontier*, similarly observed, "Lawyers are experimenting with social media to make their client's case, with George Zimmerman's defense counsel being a prime example of this."[29]

Moreover, these demands for user information are not limited to criminal cases, as corporations and others now routinely seek to reveal user-identifying information for those who post negative information anonymously to social networks, blogs and consumer gripe sites. These so-called CyberSLAPPs (Stra-

---

23. *Id*.

24. Jill Goldsmith, *One billion using Facebook*, VARIETY, Oct. 5, 2012, www.variety.com/article/VR1118060260 (noting "[Facebook's] reach can't be overstated. It added 200 million users over the past year. Some 600 million of them use Facebook on their mobile phones.").

25. *See* Yu, *supra* note 22.

26. Frances Robles, *Zimmerman defense looking for new clues on Trayvon*, MIAMI HERALD, Sept. 10, 2012, http://www.miamiherald.com/2012/09/09/2994307/zimmerman-defense-looking-for.html#storylink=misearch (noting that defense lawyers believe that, because prosecutors viewed Zimmerman's social media sites, "it's only fair game for Trayvon to undergo the same scrutiny").

27. *Id.*

28. *Id.*

29. Nicole Black, *Legal Loop: Model jury instructions discourage social media use*, THE DAILY RECORD, (Sept. 3, 2012, 10:52 PM), http://nydailyrecord.com/blog/2012/09/03/legal-loop-model-jury-instructions-discourage-social-media-use/.

tegic Lawsuit Against Public Participation) pose a very real threat to anonymous online speech.[30] In the CyberSLAPP context, the individual or organization who has been criticized has a "frivolous lawsuit" that enables them to issue subpoenas to the offending website or internet service provider (ISP). The suit thus enables them to find out who has made the comments and potentially to force them to delete their comments or otherwise "silence them."[31] In short, posters who thought their reviews were anonymous may find themselves as litigants in a CyberSLAPP case.[32]

All of these instances paint a grim picture for online privacy today. Equally troubling is the fact that the key law governing privacy in cyberspace in the United States, the Electronic Communications Privacy Act,[33] was passed more than a quarter century ago. Privacy advocates argue that this twenty-six-year-old law—which establishes the boundaries for how law enforcement can obtain electronic communications—is no longer suited to the task of regulating social media.[34] As Mark Rumold, an attorney for the Electronic Frontier Foundation, aptly phrased it, "[T]he law is arcane and confusing. And there is a significant debate on what governs what."[35]

This Article examines how the expectation of privacy in cyberspace will disintegrate if current laws are not updated to reflect changes in technology and curtail the use of subpoenas and other court orders to cull private data. Part I explores the efforts by law enforcement to troll social networking sites as a standard part of criminal investigation and how effective the current laws are in protecting citizens against unmerited intrusions into their online postings. Part II examines how private individuals and corporations are using subpoenas in an at-

30. *See* CYBERSLAPP.ORG, http://www.cyberslapp.org/ (last visited Feb. 2, 2013) (noting that "CyberSLAPP" suits are "threatening to overturn the promise of anonymous online speech and chill the freedom of expression that is central to the online world," and that these cases typically involve individuals who have anonymously criticized a corporation or public figure on the Internet").

31. *Id.*

32. *See* Robert D. Richards, *Sex, Lies and the Internet: Balancing First Amendment Interests, Reputational Harm, and Privacy in the Age of Blogs and Social Networking Sites*, 8 FIRST AMEND. L. REV. 176, 204–05 & 204 n.131 (2009).

33. 18 U.S.C. § 2510–2522 (2006).

34. *See* Yu, *supra* note 22.

35. *Id.*

tempt to unmask anonymous posters in an effort to retaliate against them in court or intimidate them into silence. Part III discusses how user agreements, or terms of service, by online providers might be used as a vehicle for safeguarding online posters by prescribing a set of core protections. Finally, the Article concludes by suggesting a framework for a comprehensive overhaul of the nation's outdated privacy laws.

I. CRIMINAL INVESTIGATIONS AND CURRENT PRIVACY LAW: ARE THE PROTECTIONS OUTDATED?

As the ACLU is fond of pointing out, "In 1986, there was no World Wide Web, nobody carried a cell phone, and the only 'social networking' two-year-old Mark Zuckerberg was doing was at pre-school or on play dates."[36] The year 1986 was not chosen at random. That year, Congress enacted the Electronic Communications Privacy Act (ECPA), the law that spells out protections for citizens communicating through electronic means, although those means have changed markedly in the quarter century since the measure was signed into law.[37] Moreover, although the ECPA was ostensibly designed to protect citizens against intrusions into their private transmissions, the ACLU warns that the law allows the government to go on a "shopping spree," collecting a "treasure trove" of information about an individual's identity, whereabouts, and activities.[38]

Particularly important in this arena is Title II of the ECPA, known as the Stored Communications Act (SCA).[39] The SCA "protects the privacy of the contents of files stored by service providers and of records held about the subscriber by service providers, such as subscriber name, billing records, or IP addresses."[40] The U.S. Department of Justice's (DOJ) interpreta-

36. *Modernizing the Electronic Communications Privacy Act (ECPA)*, ACLU, http://www.aclu.org/technology-and-liberty/modernizing-electronic-communications-privacy-act-ecpa (last visited Feb. 2, 2013).

37. *Id.*

38. *Id.*

39. 18 U.S.C. §§ 2701–2712 (2006).

40. *Privacy and Civil Liberties*, U.S. DEPT. OF JUSTICE, http://www.it.ojp.gov/default.aspx?area=privacy&page=1285 (last visited Feb. 2, 2013) (noting that "[t]he USA PATRIOT Act and subsequent federal enactments have clarified and updated the ECPA in light of the ongoing development of modern communications technologies and methods, including easing restrictions on law enforcement access to stored communications in some cases").

tion of the law and its drafters' intent sheds some light on why law enforcement today finds the wide latitude it enjoys in obtaining subpoenas and other court orders to uncover information stored by ISPs. The DOJ notes:

> To protect the array of privacy interests identified by its drafters, the [Act] offers varying degrees of legal protection depending on the perceived importance of the privacy interest involved. Some information can be obtained from providers with a subpoena; other information requires a special court order; and still other information requires a search warrant. In addition, some types of legal process require notice to the subscriber, while other types do not.[41]

Specifically, Section 2703 of Title 18 of the United States Code spells out the obligations of the parties and the courts when the government seeks to compel disclosure of information. In brief, if the information sought is "in electronic storage in an electronic communications system for one hundred and eighty days or less," then the government must obtain a warrant pursuant to state or federal law.[42] If the information has been in electronic storage for more than one hundred and eighty days, the government can obtain a court order compelling a provider of electronic communications services (ECS) or a provider of remote computing services (RCS) to disclose the contents of "any wire or electronic communication" that Section 2703 applies to.[43] Additionally, the government can obtain non-content information from an ECS or RCS through a court order.[44]

Furthermore, the SCA also allows for voluntary disclosure of content information by service providers. Under Section 2702(b), a service provider may disclose the contents of a communication to the addressee or the intended recipient, to someone authorized to forward the communication, and, in certain cases, to law enforcement.[45]

---

41. *Id*.

42. 18 U.S.C. § 2703(a) (2006).

43. *Id.* § 2703 (b). 18 U.S.C. § 2703(b)(2) provides that this part of the Statute applies to any wire or electronic communication "that is held or maintained" by an ECS or RCS on behalf of one of their subscribers and "solely for the purpose of providing storage or computer processing services" to the subscriber if the ECS or RCS does not otherwise have access to the communications. *Id.*

44. *Id.* § 2703(c).

45. *Id.* § 2702(b).

Notably, the SCA also allows service providers to disclose communications to a government entity "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury" requires such disclosure.[46] This "emergency" provision of Section 2702(b) was not part of the original Act. It was added "in response to heightened national security concerns following September 11th. This emergency provision was intended to give law enforcement more potent tools to detect and prevent crime.[47] Congress did attempt to provide a safeguard against abuses of voluntary disclosures under Section 2702 by mandating that the Attorney General file a report annually with the appropriate congressional committees detailing the number of voluntary disclosures sent to the Justice Department.[48]

The SCA played a pivotal role in the Twitter case involving Malcom Harris, the "Occupy Wall Street" protester. On January 30, 2012, Twitter informed Harris that his Twitter account, containing his user information, and his Tweets over a roughly three-month period had been subpoenaed.[49] The following day Harris notified Twitter that he would file a motion to quash the subpoena."[50] The move prompted Twitter to refrain from turning over any information until the court ruled on Harris's motion.[51]

On April 20, 2012, the court ruled against Harris, finding that Harris had no standing to challenge the subpoena.[52] To that end, the court examined Twitter's terms of service, to which users must agree before employing the social networking service. The court observed:

> The Privacy Policy informs users about the information that Twitter collects upon registration of an account and also

---

46. *Id.* § 2702(b)(8).

47. Brendan J. Coffman, *Using Clean Hands to Justify Unclean Hands: How the Emergency Exception Provision of the SCA Misapplies an Already Controversial Doctrine,* 1 N.Y.U. INTELL. PROP. & ENT. L. LEDGER, 48, 74 (2010). When the Homeland Security Act passed in Nov. 2002, "Congress included a requirement that the communication disclosed through Section 2702(b)(8) 'relate to the emergency' but also expanded the ISPs' options by allowing them to disclose to any federal, state or local government entity instead of strictly a law enforcement official." *Id.* at 75.

48. *Id.* at 76.

49. People v. Harris, 945 N.Y.S.2d 505, 506 (N.Y. Crim. Ct. 2012).

50. *Id.* at 507.

51. *Id.*

52. *Id.* at 508, 510.

> whenever a user uses Twitter's services. Twitter collects many types of user information, including IP address, physical location, browser type, mobile carrier among other types. By design, Twitter has an open method of communication. It allows its users to quickly broadcast up-to-the-second information around the world. The Tweets can even become public information searchable by the use of many search engines. Twitter's Privacy Policy informs users that, "[w]hat you say on Twitter may be viewed all around the world instantly."[53]

Although the court recognized that "New York courts have yet to specifically address whether a criminal defendant has standing to quash a subpoena issued to a third-party online social networking service seeking to obtain the defendant's user information and postings," it drew an analogy to bank record cases, in which "courts have consistently held that an individual has no right to challenge a subpoena issued against the third-party bank."[54] In short, because the bank, not the customer, owns the records, the defendant has no standing to quash a subpoena seeking production of the individual's bank records directly from the third-party bank.[55]

The court did not end its analysis on the issue of standing there. The court went on to express its failure to be persuaded by Harris's argument that he maintained a privacy interest in the material being sought. The judge noted that the defendant's assertion of privacy interests in his Tweets was "understandable, but without merit."[56] Further, borrowing liberally from a passage written by privacy scholar Orin S. Kerr on the Stored Communications Act,[57] the court observed:

---

53. *Id.* at 507.

54. *Id.* at 507–08.

55. *Id.* at 508.

56. *Id.*

57. 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, 1209–10 (2004) ("The Fourth Amendment offers strong privacy protections for our homes in the physical world. Absent special circumstances, the government must first obtain a search warrant based on probable cause before searching a home for evidence of crime. When we use a computer network such as the Internet, however, a user does not have a physical "home," nor really any private space at all. Instead, a user typically has a network account consisting of a block of computer storage that is owned by a network service provider, such as America Online or Comcast. Although a user may think of that storage space as a "virtual home," in fact that "home" is really just a block of ones and zeros stored somewhere on somebody

> The widely believed (though mistaken) notion that any disclosure of a user's information would first be requested from the user and require approval by the user is understandable, but wrong. While the Fourth Amendment provides protection for our physical homes, we do not have a physical "home" on the Internet. What an Internet user simply has is a network consisting of a block of computer storage that is owned by a network service provider. As a user, we may think that storage place to be like a "virtual home," and with that strong privacy protection similar to our physical homes. However, that "home" is a block of ones and zeros stored somewhere on someone's computer. As a consequence, some of our most private information is sent to third parties and held far away on remote network servers.[58]

Essentially, the court found that the user gives Twitter a license "to distribute that information to anyone, any way and for any reasons it chooses."[59]

Despite finding that Harris lacked standing to challenge the subpoena and that he did not retain a proprietary interest in his account's content, the court was compelled to address the application of the Stored Communications Act.[60] First, the court found that Twitter "is a service provider of electronic communication."[61] Second, the government's subpoena permitted the government "to compel disclosure of the basic subscriber and session information listed" in the Act.[62] Third, "the subpoena adhered to all of the SCA's pertinent provisions."[63] With respect to the content of Harris's Tweets, the court ruled:

> This court order will also compel Twitter to disclose @destructuremal account's Tweets, pursuant to 18 USC § 2703(d). In order to obtain the court order found in § 2703(d), the People must offer "specific and articulable facts showing that there are reasonable grounds to believe" that the Tweets "are relevant and material to an ongoing

---

else's computer. This means when we use the Internet, we communicate with and through that remote computer to contact other computers. Our most private information ends up being sent to private third parties and held far away on remote network servers.") (internal citations omitted).

58. *Harris*, 945 N.Y.S.2d at 509.

59. *Id.*

60. *Id.* at 511.

61. *Id.*

62. *Id.*

63. *Id.* at 512.

> criminal investigation." (18 USC § 2703[d]). This court finds that the factual showing has been made.[64]

Shortly after the court issued its ruling, Twitter filed a motion to quash the order with respect to the compelled disclosure of Harris's tweets pursuant to Section 2703(d).[65] Twitter argued that the court's order "imposes an undue burden upon it for at least three reasons."[66] First, Twitter proposed, the court's assertion that Harris had "no proprietary interest in the content that he submits to Twitter" was contradictory to the social network's Terms of Service, which "unequivocally state that its users 'retain [their] rights to any Content [they] submit, post or display on or through' Twitter."[67] Moreover, Twitter maintained that the SCA "expressly permits users to challenge demands for their account records."[68] The burden therefore would be upon Twitter to step in and fight for its users' rights when the order forecloses the users' ability to do so themselves.

Second, Twitter contended that it was burdened by the court's order because the order forces the social network to violate federal law.[69] Twitter relied on *United States v. Warshak*,[70] in which the Sixth Circuit held "that a subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored

---

64. *Id.* The court went on to explain how the People met the factual showing:

> In the response to the defendant's motion, the People state that the information sought by the subpoena is needed to refute the defendant's anticipated defense, that the police either led or escorted the defendant into stepping onto the roadway of the Brooklyn Bridge. The People claim the defendant's anticipated defense is contradicted by his public statements, which identifies the @destructuremal account as likely belonging to the defendant and indicates that while on the Brooklyn Bridge the defendant may have posted Tweets that were inconsistent with his anticipated trial defense. *Id.*

65. Memorandum in Support of Non-Party Twitter, Inc.'s Motion to Quash § 2703(d) Order at 1, People v. Harris, No. 2011NY080152 (N.Y. Crim. Ct., May 7, 2012) (noting that, under Section 2703(d),"'[a] court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if . . . compliance with such order otherwise would cause an undue burden on such provider'") [hereinafter Motion to Quash] (on file with author).

66. *Id.*

67. *Id.* at 1–2.

68. *Id.* at 2 (citing 18 U.S.C. § 2704(b) (2006)).

69. *Id.*

70. 631 F.3d 266 (6th Cir. 2010).

with, or sent or received through, a commercial ISP."[71] Consequently, the *Warshak* Court required authorities to obtain a warrant based upon probable cause before it would compel an ISP to turn over such content.[72] Moreover, the court found the SCA to be unconstitutional "to the extent that the SCA purports to permit the government to obtain such emails warrantlessly."[73]

Twitter argued that even if the court opted not to follow the Sixth Circuit's ruling in *Warshak*, the SCA requires a warrant when the content is less than 180 days old. Here, the court's order "compel[led] Twitter to shortly produce a multitude of content that will not be more than 180 days old until [later that] summer."[74]

Finally, on a procedural point, Twitter argued that "a criminal litigant cannot compel production of documents from a California resident like Twitter without presenting the appropriate certification to a California court, scheduling a hearing and obtaining a California subpoena for production."[75]

New York Criminal Court Judge Matthew A. Sciarrino, Jr. acknowledged that the case was one of first impression, and that it was "distinctive" because it was a criminal, rather than civil case. Moreover, the case was unusual in that the movant was a corporation, as opposed to an individual.[76] Perhaps more importantly, the case involved public postings, rather than an e-mail or text sent to one individual or a few specific individuals.[77]

The court, however, was not moved by Twitter's argument that it would be unduly burdened if it were forced to either turn over the information sought or else challenge the subpoena on behalf of its users. On that point, the court noted that the "burden is placed on *every* third-party respondent to a subpoena and cannot be used to create standing for a defendant where none exists."[78] Moreover, the court found that its order

71. *Id.* at 288 (internal quotations omitted).
72. *Id.*
73. *Id.*
74. Motion to Quash, *supra* note 65, at 2.
75. *Id.* at 3 (citations omitted).
76. People v. Harris, 949 N.Y.S.2d 590, 591 (N.Y. Crim. Ct. 2012).
77. *Id.*
78. *Id*. at 593 (citations omitted).

was "not unreasonably burdensome to Twitter, as it does not take much to search and provide data to the court."[79]

Examining the Fourth Amendment question as to whether a warrant is required, the court distinguished the recent Supreme Court decision in *United States v. Jones*, in which the Supreme Court found that attaching a Global Positioning System (GPS) tracking device to a vehicle constituted a physical invasion into a constitutionally protected area.[80] In contrast, "in this case there was no *physical* intrusion into the defendant's Twitter account. The defendant had purposely broadcast to the entire world into a server 3,000 miles away."[81]

With respect to the SCA provisions, the court looked to the dates of the requested material, measured them against the 180-day cut-off period specified in the Act, and found that "[t]he non-content records such as subscriber information, logs maintained by the network, server, etc. and the September 15, 2011 to December 30, 2011 tweets are covered by the court order. However, the government must obtain a search warrant for the December 31, 2011 tweets."[82]

In the opinion, Judge Sciarrino also acknowledged that as social media continues to evolve, "judges are asked to make decisions based on statutes that can never keep up with technology."[83] Despite unclear or arcane policy, the *Harris* court found that judges have an obligation to work through these issues. In his parting salvo, Judge Sciarrino wrote:

> Judges must then do what they have always done—balance the arguments on the scales of justice. They must weigh the interests of society against the inalienable rights of the individual who gave away some rights when entering into the social contract that created our government and the laws that we have agreed to follow. Therefore, while the law regarding social media is clearly still developing, it can neither be said that this court does not understand or appreciate the place that social media has in our society nor that it does not appreciate the importance of this ruling and future rulings of courts that may agree or disagree with this decision. In

79. *Id.* at 593–94.
80. 132 S. Ct. 945, 946 (2012).
81. *Harris*, 949 N.Y.S.2d at 594.
82. *Id.* at 596.
83. *Id.* at 597.

> recent years, social media has become one of the most prominent methods of exercising free speech, particularly in countries that do not have very many freedoms at all.[84]

Although some online devotees might welcome the court's sentiment toward the value of social media, Malcolm Harris likely found little comfort in the decision. Still, Twitter stepped in and challenged the subpoena—something not every social networking company would be inclined to do. The Electronic Frontier Foundation, an organization devoted to championing "the public interest in every critical battle affecting digital rights,"[85] praised Twitter in its 2012 report entitled "When the Government Comes Knocking, Who Has Your Back?" for upgrading its practices in the past year.[86] The privacy rights organization specifically singled out Twitter's resistance to the government's subpoena in the Harris case.[87]

As mentioned above, Twitter has adopted "Guidelines for Law Enforcement," which advise that Twitter requires "a subpoena, court order, or other valid legal process" in order for Twitter to disclose information about its users.[88] Moreover, Twitter maintains that it will notify users of any request for information before handing over the information unless prohibited from doing so by statute or court order.[89]

Facebook's "Information for Law Enforcement Authorities" mirrors the disclosure requirements under the Stored Communications Act, stating that Facebook "may disclose" user information pursuant to a subpoena, court order, or other request.[90] LinkedIn[91] and Dropbox[92] follow a similar approach. Moreover,

---

84. *Id*.

85. *About EFF*, ELEC. FRONTIER FOUND., https://www.eff.org/about (last visited Oct. 19, 2012) (noting that "EFF broke new ground when it was founded in 1990—well before the Internet was on most people's radar—and continues to confront cutting-edge issues defending free speech, privacy, innovation, and consumer rights today").

86. *See When the Government Comes Knocking, Who Has Your Back?*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/who-has-your-back (last visited Feb. 2, 2013).

87. *See id*.

88. *Guidelines for Law Enforcement*, *supra* note 7.

89. *Id*.

90. *See Law Enforcement & Third-Party Matters*, *supra* note 8.

91. *See* LINKEDIN, LINKEDIN LAW ENFORCEMENT DATA REQUEST GUIDELINES, *supra* note 9.

92. *See Law Enforcement Handbook*, *supra* note 10.

all of those social networks provide some exception for emergencies or to prevent fraud or illegality.[93]

Increased privacy vigilance on the part of social networks, including the development of specific standards for safeguarding user information, is now imperative. As the Electronic Frontier Foundation observed, "There is no question that law enforcement is eagerly accessing location information from third-party providers for a wide range of investigations. It's vital these providers commit to being transparent about government access requests and fighting those requests when they are overbroad."[94]

II. CIVIL LAWSUITS AND THE BURGEONING THREAT TO ANONYMOUS ONLINE SPEECH

The observation by the attorney for "Occupy Boston" protester Guido Fawkes that "most users of Twitter and other social networks would 'reasonably expect' their speech is anonymous"[95] soon may sound profoundly naïve. Although criminal cases involving investigations that uncover user information have garnered a fair amount of attention, civil lawsuits strategically designed to elicit similar material have largely flown under the journalistic radar of the daily news cycle. Nonetheless, in terms of privacy loss, the results of such lawsuits can be equally, if not more, devastating because they threaten to unravel the centuries-long tradition of anonymous speech in this country. Without question, an author's ability to speak anonymously is a privacy value that finds its roots in the Constitution.[96]

The decision to speak anonymously is one that cannot be separated from the basic right of free expression safeguarded by the First Amendment.[97] In *McIntyre v. Ohio Elections Commis-*

93. *See Law Enforcement & Third-Party Matters*, *supra* note 8; LINKEDIN, LAW ENFORCEMENT DATA REQUEST GUIDELINES, *supra* note 9; *Law Enforcement Handbook*, *supra* note 10.

94. *When the Government Comes Knocking, Who Has Your Back?*, *supra* note 86.

95. Shalvey, *supra* note 11.

96. *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995) (finding author's decision to remain anonymous rooted in First Amendment); Doe v. 2TheMart.com, Inc., 140 F. Supp. 2d 1088, 1092 (W.D. Wash. 2001) (stating that "[t]he right to speak anonymously was of fundamental importance to the establishment of our Constitution," and that this right extends to "speech via the internet").

97. U.S. CONST. amend I (providing, in pertinent part, that "Congress shall make no law . . . abridging freedom of speech, or of the press").

sion, the Supreme Court stated that "an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment."[98] Citizens have been motivated to hide their identities throughout history, and, as the *McIntyre* Court suggested, "[t]he decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely a desire to preserve as much of one's privacy as possible."[99]

The Internet brought new challenges, as anonymous posting has become more commonplace and has therefore raised new, complex legal issues that challenge existing legal doctrine.[100] The subject of postings containing negative messages often wants to know who is instigating the attack. In *Doe v. 2TheMart.com, Inc.*, one of the earliest reported decisions dealing with a motion to quash a subpoena issued on a local Internet service provider in an effort to uncover the identity of an anonymous poster, U.S. District Court Judge Thomas S. Zilly pointed out the significance of the case: "The motion raises important First Amendment issues regarding Doe's right to speak anonymously on the Internet and to proceed in this Court using a pseudonym in order to protect that right."[101] The matter also immediately raised First Amendment concerns because "[a] court order, even when issued at the request of a private party in a civil lawsuit, constitutes state action and as such is subject to constitutional limitations."[102]

The court traced the long tradition of anonymous speech in this country, recognizing that in early American history, anonymous speech, including the use of pseudonyms, was a "powerful tool[] of political debate."[103] As a result, it is only logical to extend that tradition to the most powerful communication tool yet invented—the Internet. To that end, Judge Zilly concluded, "The right to speak anonymously extends to speech via the Internet. Internet anonymity facilitates the rich, diverse,

98. 514 U.S. at 342.
99. *Id.* at 341–42.
100. 2TheMart.com, 140 F. Supp. 2d at 1091.
101. *Id.* at 1089.
102. *Id.* at 1091–92.
103. *Id*. at 1092.

and far ranging exchange of ideas."[104] That settled, it has become incumbent upon Judge Zilly and other judges around the country to fashion a legal test that secures the right to post anonymously in an online forum, for, as Judge Zilly aptly observed: "If Internet users could be stripped of that anonymity by a civil subpoena enforced under the liberal rules of civil discovery, this would have a significant chilling effect on Internet communications and thus on basic First Amendment rights."[105]

A. The Dendrite/Cahill *Construct*

In the absence of Supreme Court guidance on the specific issue of online anonymity, lower courts were forced to develop their own standards that would balance the rights of the anonymous poster against those of the target of the negative post. Two cases, one from New Jersey and the other from Delaware, became the standard bearers that other courts would look to as models for handling the issue.

In *Dendrite Int'l, Inc. v. Doe, No. 3*,[106] the court recognized that trial courts must balance the First Amendment right to speak anonymously against the plaintiff's right to protect her "interests and reputation" by bringing claims against "anonymous, fictitiously-named defendants."[107] To accomplish that balance, the court created a four-pronged approach, topped off by the critical notion of notice. First, the plaintiff must try to notify the anonymous posters that they are the subject of court action and thereby provide the defendants a reasonable opportunity to respond.[108] Second, the plaintiff must identify the exact statements made by each anonymous poster that the plaintiff considers objectionable speech.[109] Third, the plaintiff must provide enough evidence to support a prima facie case against the unnamed defendants before a court orders the defendant to reveal his identity.[110] Finally, assuming the plaintiff has established the prima facie case, "the court must balance the defendant's First Amendment right of anonymous free speech

104. *Id.*
105. *Id.* at 1093.
106. 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001).
107. *Id.* at 760.
108. *Id.*
109. *Id.*
110. *Id.*

against the strength of the prima facie case presented and the necessity for the disclosure of the anonymous defendant's identity to allow the plaintiff to properly proceed."[111]

Subsequently, the Delaware Supreme Court in *Doe No. 1 v. Cahill*[112] observed that "[a]nonymous internet speech in blogs or chat rooms in some instances can become the modern equivalent of political pamphleteering,"[113] and therefore requires protection. Because of its concern that a low standard for finding online posters liable would have a chilling effect on Internet free speech, the court required the plaintiff to satisfy a "summary judgment standard" before uncovering the identity of an anonymous online poster who had become the subject of legal action.[114] The *Cahill* court examined the *Dendrite* ruling and found that imposing a summary judgment standard on the party seeking to unmask the poster obviates the need for *Dendrite* prongs two and four:

> The second requirement, that the plaintiff set forth the exact defamatory statements, is subsumed in the summary judgment inquiry. To satisfy the summary judgment standard a plaintiff will necessarily quote the defamatory statements in his complaint. The fourth *Dendrite* requirement, that the trial court balance the defendant's First Amendment rights against the strength of the plaintiff's *prima facie* case is also unnecessary. The summary judgment test is itself the balance.[115]

In short, the *Cahill* court adopted a "modified *Dendrite* standard consisting only of *Dendrite* requirements one and three: the plaintiff must make reasonable effort to notify the defendant and must satisfy the summary judgment standard."[116]

Although *Dendrite* and *Cahill* serve as basic models, other courts have adopted portions of each to fashion their own tests.[117] For instance, in *Mobilisa, Inc. v. John Doe 1*,[118] the Arizona Court of Appeals embraced the notice requirements pre-

---

111. *Id.* at 760–61.

112. 884 A.2d 451 (Del. 2005).

113. *Id.* at 456.

114. *Id.* at 457 (internal quotation marks omitted).

115. *Id.* at 461.

116. *Id.*

117. *See, e.g.*, Indep. Newspapers, Inc. v. Brodie, 966 A.2d 432, 457 (Md. 2009) (adopting a five-part test that encompasses the *Dendrite* standard).

118. 170 P.3d 712 (Ariz. Ct. App. 2007).

sent in both *Dendrite* and *Cahill*.[119] *Mobilisa* rejected the standard of simply requiring a plaintiff to set forth a prima facie case on the rationale that it would chill anonymous Internet speech. Instead, the court adopted the summary judgment standard from *Cahill*.[120] But the court disagreed with *Cahill*'s conclusion that no balancing step was needed, so it adopted the fourth *Dendrite* prong.[121] The court found that this step "furthers the goal of compelling identification of anonymous internet speakers only as a means to redress legitimate misuses of speech rather than as a means to retaliate against or chill legitimate uses of speech."[122]

In *Faconnable USA Corp. v. John Does 1-10*,[123] a U.S. Magistrate Judge in Colorado admitted that he was "unaware of a substantial body of law in other jurisdictions addressing First Amendment concerns and the issuance of John Doe subpoenas like those requested here."[124] Magistrate Judge Boyd N. Boland decided that he simply needed to "assure that the disclosure of the anonymous posters' identities (1) serves a substantial governmental interest and (2) is narrowly tailored to serve that interest without unnecessarily interfering with First Amendment freedoms."[125] He found the first requirement satisfied: the government has a substantial interest in allowing plaintiffs with non-frivolous claims to assert their rights against anonymous Internet posters.[126] Because the subpoena sought to uncover the identities of anonymous posters, Judge Boland found that it was narrowly tailored to serve that interest.[127] The magistrate's order was, however, rendered moot because the plaintiff sought a voluntary dismissal of the action. Further, the district court vacated it because the Internet service provider, on behalf of the "John Doe Defendants," "had nothing to do with causing

119. *Id.* at 719.
120. *Id.* at 720.
121. *Id.*
122. *Id.*
123. No. 11-cv-00941-CMA-BNB, 2011 U.S. Dist. LEXIS 56303 (D. Colo. May 24, 2011).
124. *Id.* at *3.
125. *Id.* at *22.
126. *Id.* at *22–23.
127. *Id.* at *23.

its objections to become moot, [and] it 'ought not in fairness be forced to acquiesce' in the Magistrate Judge's Order."[128]

Thus, a patchwork of standards governs the anonymous-poster subpoena cases throughout the nation. As Professor Lyrissa Lidsky has noted, "The development of appropriate standards to govern the John Doe cases has been and continues to be a piecemeal process, developing case-by-case and court-by-court."[129] First Amendment advocates should be concerned by these developments.

One point is clear: These balancing tests are critical to ensuring that plaintiffs are not engaging in a fishing expedition solely designed to ferret out and punish potential defendants for speaking out. Professor Lidsky has subscribed to this idea as well: "Put simply, these standards, or balancing tests, are designed to sort legitimate defamation actions from 'cyber-slapps'—unfounded suits designed only to chill speech—at an early stage of the discovery process."[130]

B. CyberSLAPPs: Squelching Speech Through Intimidation

On August 2, 2012, then-Senator Jon Kyl introduced a bill "[t]o protect first amendment rights of journalists and internet service providers by preventing States and the United States from allowing meritless lawsuits arising from acts in furtherance of those rights."[131] Significantly, one of the provisions in the bill provides:

> A person whose personally identifying information is sought in connection with a claim that arises in whole or in part from an oral or written statement or other expression that is on a matter of public concern or that relates to a public official or figure, or a person from whom such information is sought in connection with such a claim, may file a

128. Faconnable USA Corp. v. John Does 1-10, 799 F. Supp. 2d 1202, 1204 (D. Colo. 2011).

129. Lyrissa Barnett Lidsky, *Anonymity in Cyberspace: What Can We Learn from John Doe?*, 50 B.C. L. REV. 1373, 1385 (2009) (noting that "[w]hen the law is asked to solve a problem created by new technology, it is hard for the law to 'get it right' unless decisionmakers understand not just the technology, but the social and cultural uses of the technology as well").

130. *Id.* at 1376–77.

131. Free Press Act of 2012, S. 3493, 112th Cong. (2011).

> special motion to quash the request or order to produce the information.[132]

This is a special acknowledgement to CyberSLAPPs, a type of lawsuit that threatens to chill online freedom of expression. Typically, CyberSLAPP cases involve a person who has anonymously criticized a corporation or public figure on the Internet.[133] The CyberSLAPP filer then uses a subpoena to identify potential defendants to sue.[134] The special motion to quash the subpoena or other court order would be a vital tool in tamping down this misuse of process.

Nonetheless, advocacy groups lobbying in favor of federal anti-SLAPP protection had hoped for a more expansive treatment of the issue. Evan Mascagni, organizer and legislative assistant of the Public Participation Project,[135] a group that has been leading the efforts toward a federal solution, wrote:

> While the Public Participation Project applauds Senator Kyl's efforts to enact federal anti-SLAPP legislation before he retires at the end of this term, PPP does not endorse this bill because of its narrow scope. Essentially, the bill has two components—a very narrow anti-SLAPP provision that only applies to representatives of the news media, and a broader special motion to quash subpoenas for personally identifying information in connection with a claim arising from statements on a matter of public concern or that relate to a public official or public figure.[136]

The Public Participation Project has been pushing proposed legislation called the PETITION Act, a measure that would apply to the broader spectrum of SLAPP targets and would sweep bloggers and other citizens who speak out on issues under its

---

132. *Id*. § 4205(a).

133. *See* CyberSLAPP.org, *supra* note 30.

134. *See* CyberSLAPP.org, *supra* note 30 and accompanying text.

135. *See* PUBLIC PARTICIPATION PROJECT, http://www.anti-slapp.org (last visited Feb. 4, 2013) (noting that "[t]he Public Participation Project works to protect citizens from lawsuits designed to chill their ability to communicate with their government or speak out on issues of public interest. Such lawsuits, called Strategic Lawsuits Against Public Participations (SLAPPs), pose serious dangers to free expression throughout the country. The Public Participation Project is working to enact legislation in Congress to provide protection from these lawsuits.").

136. Evan Mascagni, *Free Press Act of 2012*, PUBLIC PARTICIPATION PROJECT, http://www.anti-slapp.org/recent/free-press-act-of-2012 (last visited Feb. 4, 2013).

protection.[137] Representative Steve Cohen of the 111th Congress introduced an earlier version of this measure as the Citizens Participation Act of 2009.[138] Importantly, Representative Cohen's bill also contained protection from those who seek personal identifying information from Internet Service Providers.[139]

In August 2012, the American Bar Association adopted a resolution encouraging state and federal lawmakers "to enact legislation to protect individuals and organizations who choose to speak out on matters of public concern from meritless litigation designed to suppress speech, commonly known as SLAPPs (Strategic Lawsuits Against Public Participation)."[140] The report accompanying the resolution noted that "[t]he proposed federal statute also provides for a 'special motion to quash,' protecting anonymous speakers from having their identities revealed through discovery or subpoena, unless a plaintiff can show that the underlying case has merit."[141]

Although thirty states and the District of Columbia have varying degrees of protection for SLAPP targets,[142] California became the first to amend its law to specifically guard against cyberSLAPPs and the practice of using a subpoena or court order against an ISP to reveal potential defendants.[143] After then-

---

137. *See The Petition Act*, PUBLIC PARTICIPATION PROJECT, http://www.anti-slapp.org/the-citizen-participation-act-h-r-4364/ (last visited Feb. 4, 2013) (specifying that "[a]n anonymous speaker whose personally identifying information is sought in a subpoena or discovery order because he/she has petitioned the government or spoken out on a public issue, may make a special motion to quash that discovery order or subpoena. In addition, the individual, or entity, from which such information is sought may also file a motion to quash. If the plaintiff in the underlying case cannot show that the underlying case has merit, the subpoena must be quashed.").

138. *See* Citizen Participation Act of 2009, H.R. 4364, 111th Cong. (1st Sess. 2009).

139. *Id.* § 7(a), § 11(6).

140. AM. BAR ASSOC., RESOLUTION ADOPTED BY HOUSE OF DELEGATES (2012) (on file with author).

141. *Id.* at 1.

142. *See State Anti-SLAPP Laws*, PUBLIC PARTICIPATION PROJECT, http://www.anti-slapp.org/your-states-free-speech-protection (last visited Feb. 4, 2013) (noting that twenty-eight states and the District of Columbia have enacted legislation); *See also* Protect Our Mountain Envt., Inc. v. District Ct., 677 P.2d 1361, 1366–67 (Colo. 1984); Webb v. Fury, 282 S.E.2d 28, 33 (W. Va. 1981) (noting that West Virginia and Colorado, respectively, have anti-SLAPP-like protections in their case law).

143. Cal. Civ. Proc. Code § 1987.1 (West 2008) (providing, in pertinent part: "(a) If a subpoena requires the attendance of a witness or the production of books, documents, or other things before a court, or at the trial of an issue therein, or at

California Governor Arnold Schwarzenegger signed Assembly Bill 2433 into law, the Electronic Frontier Foundation heralded the measure.[144] That organization noted:

> One of the most pernicious threats to anonymity is the filing of trumped-up lawsuits as an excuse to force ISPs to reveal speakers' identities. Once such a lawsuit is filed, speakers who want to protect their anonymity must find a way to pay a lawyer to go to court and prevent disclosure of their personal information. That can be a real hardship—in fact, even the threat of having to go to court may discourage many people from speaking out in the first place.[145]

One legal commentator characterized the problem this way:

> A CyberSLAPP subpoena threatens to deprive John Doe of his right to speak anonymously without notice, judicial review, or any credible evidence of the claims against him. This is particularly troublesome because many cyberSLAPP plaintiffs seek only to discover John Doe's identity, not to obtain a judgment against him. In such cases, without meaningful notice and substantive review of the plaintiff's claim, the game is over before John Doe even knows it has begun.[146]

Other states currently introducing anti-SLAPP bills or amending existing laws should consider special protections for users of social networks and anonymous speakers, including mechanisms that would challenge subpoenas designed to re-

---

the taking of a deposition, the court, upon motion reasonably made by any person described in subdivision (b), or upon the court's own motion after giving counsel notice and an opportunity to be heard, may make an order quashing the subpoena entirely, modifying it, or directing compliance with it upon those terms or conditions as the court shall declare, including protective orders. In addition, the court may make any other order as may be appropriate to protect the person from unreasonable or oppressive demands, including unreasonable violations of the right of privacy of the person; (b) The following persons may make a motion pursuant to subdivision (a): . . . (5) *A person whose personally identifying information, as defined in subdivision (b) of Section 1798.79.8 of the Civil Code, is sought in connection with an underlying action involving that person's exercise of free speech rights*) (emphasis added).

144. Corynne McSherry, *California Governor Signs Off on New Protections for Free Speech*, ELEC. FRONTIER FOUND., Oct. 2, 2008, https://www.eff.org/deeplinks/2008/10/california-governor-signs-new-protections-free-spe.

145. *Id.*

146. Shaun B. Spencer, *CyberSLAPP Suits and John Doe Subpoenas: Balancing Anonymity and Accountability in Cyberspace*, 19 J. MARSHALL J. COMPUTER & INFO. L. 493, 519 (2001) (stating that "the abuse of cyberSLAPP claims today may leave future victims of online defamation without a remedy").

veal a poster's identity. In August 2010, for instance, the Michigan House of Representatives passed a bill that provided protections for postings on social networking sites, including Facebook and Twitter."[147] After passage by the House, however, the bill stalled in the Senate.[148] Nonetheless, safeguarding electronic communications from frivolous cases in the age of social networks not only protects freedom of speech but also, given the high usage of social media, keeps court dockets free of potential nuisance lawsuits.

Anti-SLAPP laws also can help in a very practical way in cases where the identity of an anonymous poster is sought. One of the key provisions in a well-crafted anti-SLAPP law provides for "[l]imits or stays on discovery while the court considers a motion to dismiss under the anti-SLAPP law."[149] If states would automatically stay discovery upon filing of a motion to strike or special motion to dismiss under their anti-SLAPP laws, this automatic stay would obviate the need to file a separate motion to quash the subpoena seeking the identifying information. The anonymous speaker would be protected while the motion is pending. If the court finds that the lawsuit qualifies as a SLAPP, then the poster's identity would remain safeguarded. If, on the other hand, the court finds the lawsuit has merit, then it could engage in a *Dendrite-Cahill*-type analysis to determine if the speaker's identity should be revealed.

---

147. *Michigan bill aims to stop some harassment suits*, MLIVE.COM, Aug. 19, 2010, http://www.mlive.com/news/index.ssf/2010/08/michigan_bill_aims_to_stop_som.html.

148. *See* MICHIGAN LEGISLATIVE WEBSITE, http://www.legislature.mi.gov/(S(e0nbwanpn01pjjj44k0i5i55))/mileg.aspx?page=getObject&objectName=2009-HB-5036 (last visited Feb. 4, 2013).

149. *Responding to Strategic Lawsuits Against Public Participation (SLAPPs)*, CITIZEN MEDIA LAW PROJECT, http://www.citmedialaw.org/legal-guide/responding-strategic-lawsuits-against-public-participation-slapps (last visited Feb. 4, 2013) (describing the common components of anti-SLAPP law, including protection for speech on issues of public significance and/or activities aimed at petitioning the government for action on economic, social, and political issues; procedural mechanisms for obtaining early dismissal of a SLAPP; recovery of attorneys' fees and court costs incurred in defending against a SLAPP; and expedited review of motions to dismiss in order to reduce the time and costs of litigation).

III. POINT AND CLICK: HOW TERMS OF SERVICE CAN HELP SALVAGE USERS' REASONABLE EXPECTATIONS OF PRIVACY IN CYBERSPACE

In *People v. Harris,* Judge Sciarrino noted that Twitter had recently amended its terms of service—presumably in response to the subpoena by the Manhattan District Attorney's Office—to enable users to retain the rights to any content they post on the service.[150] The court, in part, based Harris's lack of standing on the notion that once he posted his content on Twitter, he had lost all proprietary interests in it.

In ruling against Twitter, the judge observed that:

> The court's decision was partially based on Twitter's then terms of service agreement. After the April 20, 2012 decision, Twitter changed its terms and policy effective May 17, 2012. The newly added portion states that: "You Retain Your Right To Any Content You Submit, Post Or Display On Or Through The Service."[151]

In the earlier case, in which Malcolm Harris sought the protective order himself, the court was clear that Harris had agreed to the terms of service, which granted away his rights:

> Here, the defendant has no proprietary interests in the @destructuremal account's user information and Tweets between September 15, 2011 and December 31, 2011. As briefly mentioned before, in order to use Twitter's services, the process of registering an account requires a user's agreement to Twitter's Terms. Under Twitter's Terms it states in part:
>
> > By submitting, posting or displaying Content on or through the Services, you grant us a worldwide, non-exclusive, royalty-free license to use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute such Content in any and all media or distribution methods (now known or later developed).[152]

Judge Sciarrino's April and June 2012 opinions, read together, suggest that social networks could help their users retain standing to move to quash subpoenas through carefully crafted terms of service. As privacy scholar Woodrow Hartzog

---

150. 949 N.Y.S.2d 590, 591 (N.Y. Crim. Ct. 2012).

151. *Id.* at 593.

152. People v. Harris, 945 N.Y.S.2d 505, 508 (N.Y. Crim. Ct. 2012).

has observed, "When courts seek to determine a website user's privacy expectations and the website's promises to that user, they almost invariably look to the terms of use agreement or to the privacy policy."[153] Although this would be of great use to the user, it would also serve the purposes of the social network.

In *Harris*, Twitter felt compelled to challenge the subpoena because its user was left without *any* recourse once the judge ruled that the user had given up his proprietary interests. But if social networks were to ensure that those interests remain with the user while being shared with the service, then individuals would be able to manage their own destinies rather than hope that others will take up their charge.

Of course, this notion presupposes that users are attuned enough to the social network's privacy policies and terms of service to understand what is at stake for them. Nicole A. Ozer, Technology and Civil Liberties Policy Director at the ACLU of Northern California has asked:

> If consumers do not understand how their personal information is being used, do not realize the costs of online services and the potential risks to their personal interest, are concerned that expressing a desire for privacy implies that they have "something to hide," and are therefore unwilling or unable to take individual steps to protect their personal interest, why would they come together in a social movement to collectively push for change?[154]

Indeed, Facebook's chief executive officer Mark Zuckerberg found that "an increased willingness to share personal information and decreased concern about privacy is simply a new 'social norm.'"[155]

Nonetheless, Ozer suggests that society continues to be concerned about privacy, but that "consumers have very little un-

---

153. Woodrow Hartzog, *Website Design as Contract,* 60 AM. U. L. REV 1635, 1635–36 (2011) (noting further that "[c]ourts rarely look to the privacy settings or other elements of a website where users specify their privacy preferences because these settings and elements are typically not considered part of any contract or promise to the user").

154. Nicole A. Ozer, *Putting Online Privacy Above the Fold: Building a Social Movement and Creating Corporate Change,* 36 N.Y.U. REV. L. & SOC. CHANGE 215, 224 (2012) (noting that "[i]t is now widely recognized that consumers understand very little about how the technology and services they use every day really function or how these services' privacy practices apply to their own personal information").

155. *Id.* at 223.

derstanding of the actual privacy practices of the services that they use or the legal constraints on these practices."[156] Ozer believes the continued growth and widespread use of technology, including by influential lawmakers, is moving the privacy issue into the arena of public policy debate.[157] Furthermore, she suggests that the recent economic downturn has actually forced many companies increase transparency regarding how they use consumers' personal information.[158]

Perhaps the heightened awareness and attention to the privacy issues posed by social networks on the part of both government and industry will forge an opportunity for change. As lawmakers become more concerned about their own privacy in the online world, new legislation governing the issue will likely blossom. Typically, industry self-regulation is far preferable to governmental mandates. Thus, this is a propitious moment for social networks, both individually and as a burgeoning industry, to create standards that move the protection of user privacy into the forefront of their terms of use. To date, user agreements clearly are designed to broadly immunize social networks from liability. Too often, privacy policies get lost in the several pages of legal jargon that go largely unread by consumers eager to use the service. By creating a streamlined privacy policy that offers maximum protection to the user—including retained rights in the content and a specified process for challenging subpoenas—and requiring consumers to separately read and agree to the terms of use, social networks will create a better service for their users and perhaps stave off further government intervention.

CONCLUSION

The law indisputably lags behind the growth of technology. What is becoming increasingly problematic is that technology is changing so rapidly, and becoming so much more expansive, that by the time the law absorbs a new device or service, a newer iteration of it with many more applications is already on

156. *Id.* at 224.

157. *Id.* at 234–35 (stating that "[t]he Rules of the House of Representatives were amended at the beginning of the 2011 term to allow members to use electronic devices on the House floor").

158. *Id.* at 235.

the market. Moreover, the popular technology of this generation, particularly social networks, requires the sharing of information rather than merely receiving it.[159] With that sharing paradigm comes the disclosure of personal data that can, especially in the wrong hands, cause problems for online users.

Along with this explosive growth in technology comes the potential for abuse. This Article has explored the abuses associated with the growth in social networks. That abuse comes from both government and the private sector. One point clearly emerges: These abuses demonstrate the need for reform.

The key law governing the storage and retrieval of personal information was signed into law in 1986. That fact should give all Americans pause. The Stored Communications Act, although arguably adequate at its inception, today leaves too much open to interpretation and thus provides an open invitation to law enforcement and courts to massage meaning into it which serves the purpose of the government by allowing compulsory process without properly balancing the privacy interests of its citizens. Just as the Telecommunications Act of 1996[160] comprehensively overhauled the law that previously governed communications in this country—the Communications Act of 1934[161]—the Electronic Communications Privacy Act[162] (and its component SCA) has become outdated and no longer up to the task of preserving privacy in a rapidly changing technological environment.

On the civil side of the law, all Americans should be concerned about the increased attempts by individuals and corporations to unmask the identity of anonymous posters in the online world. Legal reforms on both the state and federal levels are needed. Although legal reform is not always easy, the basis for the necessary adjustments already exists. First, states with anti-SLAPP laws should amend those measures to include specific protections against cyberSLAPPs, including an automatic stay on subpoenas issued to reveal identifying information about anonymous posters. Second, Congress should enact federal anti-SLAPP legislation with the very same safeguards. This

159. Previously, information conveyance flowed one way from sender to receiver (for example, in radio, recorded music, motion pictures, and television).

160. Pub. L. No. 104-104, 110 Stat. 56 (1996).

161. Pub. L. No. 416, 48 Stat. 1064 (1934).

162. 18 U.S.C. §§ 2510–2522 (2006).

federal law would help in those states with weak or no anti-SLAPP protections. Third, courts should work to develop a national, uniform standard with respect to the legal showing needed to reveal the identity of an anonymous poster—one that includes the utmost protection possible to safeguard the poster's identity. The patchwork of laws that now exists threatens to undermine the longstanding tradition of anonymous speech in this country.

Finally, social networks themselves can institute policy changes that would go a long way toward preserving the privacy interests of their users. They need to ensure that individuals retain a proprietary interest in the information they provide or convey through the network. These social networks must especially consider how to challenge subpoenas. Moreover, social networks should rework privacy policies so that they focus on and are comprehensible to the user. The privacy policies should be simple and separately agreed upon in an effort to educate users as to the importance of privacy protection in the online world. As noted above, ultimately these measures are a matter of sound business practice because, as lawmakers become more attuned to the loss of their own privacy in cyberspace, the more likely they are to push for heavy regulation of the social network industry.