Hastings Communications and Entertainment Law Journal

Volume 33 | Number 3 Article 7

1-1-2011

Facebook and Social Networks: the Government's Newest Playground for Information and the Laws That Haven't Quite Kept Pace

Danielle Levine

Facebook and Social Networks: the Government's Newest Playground for Information and the Laws That Haven't Quite Kept Pace

By
DANIELLE LEVINE*

I. Introduction

The Internet has, in recent decades, become the center of our world. It is where we search for information, how we keep up on current events in real time, and now, where we share copious amounts of information about ourselves. The boom of social networking websites[1] such as Facebook,[2] MySpace,[3] and Twitter[4] has allowed individuals to disseminate personal information at an alarming rate—from our basic contact information, to our interests, to photographs, and updates about our every move, and thought.

* University of California, Hastings College of the Law, J.D. Candidate 2011. Stanford University, B.A. American Studies, with Departmental Honors and Distinction, 2007. Danielle would like to thank Professor John Diamond for overseeing this paper, and her family for their unyielding love, encouragement, and support.

1. *See* James Grimmelmann, *Saving Facebook,* 94 IOWA L. REV. 1137, 1142 (2009) (Social networks are defined as "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.") (internal citation omitted).

2. FACEBOOK, http://www.facebook.com (last visited Jan. 25, 2010).

3. MYSPACE, http://www.myspace.com (last visited Jan. 25, 2010).

4. TWITTER, http://www.twitter.com (last visited Jan. 25, 2010).

With so many people uploading sensitive information to their Facebook profiles, there have been many unintended consequences—"[j]obs have been lost, reputations smeared, embarrassing secrets broadcast to the world."[5] Most significantly, however, the rise of social networks as a new medium of communication has provided a new frontier of how the government can gain access and use that information in criminal investigations and prosecutions.

On December 1, 2009, The Electronic Frontier Foundation ("EFF"), along with the Samuelson Law, Technology, and Public Policy Clinic at the University of California, Berkeley, School of Law ("Samuelson Clinic"), filed a lawsuit against several government agencies seeking the release of records under the Freedom of Information Act ("FOIA"),[6] concerning how those agencies use social-networking websites as investigative, surveillance, and data collection tools.[7] This lawsuit marks an important acknowledgment that there are not clearly defined ways in which governmental agencies take advantage of the copious amounts of data provided by social networking sites. The Samuelson Clinic also co-sponsored a conference ("Samuelson Conference") addressing the legal and ethical issues surrounding data gathering on social networking sites, the contents of which will be referred to throughout this note.[8]

The EFF's lawsuit is especially important because social networking statistics are phenomenal: Facebook has hit the three hundred million users mark, MySpace has one hundred and twenty-five million accounts, and in September 2009, Twitter had twenty million visitors.[9] Amongst the eighteen- to twenty-four-year-old demographic, almost seventy-five percent are using social networks.[10]

This Note will examine the ways in which social networking sites and the government's search for information collide. Part Two will

5. Grimmelmann, *supra* note 1, at 1140. (Noting that "[o]ver a hundred million people have uploaded personally sensitive information to Facebook, and many of them have been badly burnt as a result.")

6. Freedom of Information Act ("FOIA"), 5 U.S.C. § 552 (2010).

7. Elect. Frontier Found. v. Dept. of Defense, 2009 WL 4813489 (N.D.Cal. Dec. 1, 2009). The case also names the Central Intelligence Agency, Department of Homeland Security, Department of Justice, Department of Treasury, and Office of the Director of National Intelligence as defendants. *See also* Press Release, Electronic Frontier Foundation, *Lawsuit Demands Answers About Social-Networking Surveillance* (Nov. 30, 2009) *available at* http://www.eff.org/press/archives/2009/11/30.

8. Samuelson Conference, Social Networks: Friends or Foes? Confronting Online Legal and Ethical Issues in the Age of Social Networking (Oct. 23, 2009), *available at* http://www.law.berkeley.edu/institutes/bclt/socialnetworking/schedule.htm. [hereinafter Samuelson Conference]

look at Facebook, examining its privacy policies and how information and data are shared on the site. It will then discuss the ways in which the government has used both Facebook and similar social networking sites in its investigations. Part Three will outline the statutory framework through which the government operates to gain access to electronic data and analyze its impact by examining case law surrounding those information privacy statutes as they apply to Fourth Amendment litigation. Finally, Part Four will discuss the intersection between the law as it currently stands, and social networking sites. The law has not quite kept pace with the speed of technology. As a result, the boundaries of individual privacy—as applied to the government's use of social networking information—are in need of revisions.

II. Social Networks

Facebook's domination of the social network market makes it an ideal case study through which to demonstrate the enormous amount of information that users are able to share through the social network medium. According to the site's Privacy Policy, "[o]ne of the primary reasons people use Facebook is to share content with others."[11]

Facebook users share and display a vast amount of content. Facebook users complete profiles that can contain up to about forty pieces of recognizable personal information.[12] This includes "name, birthday, political and religious views; online and offline contact information; gender, sexual preference, and relationship status; favorite books, movies, and so on; educational and employment history; and, of course, picture[s]."[13] It has been further noted that Facebook is storing over twenty billion photos.[14] What is more alarming is that Facebook's users share this information with thousands of others—information which is "indexed to create powerful mosaics of personal data."[15]

9. David Lee, *Problems Unique to Social Networking and the Law*, address at Samuelson Conference, (Oct. 23, 2009), *available at* http://www.law.berkeley.edu/7458.htm.

10. *Id.*

11. *See Privacy Policy (Facebook), available at* http://www.facebook.com/policy.php (last visited Jan. 25, 2010).

12. Grimmelmann, *supra* note 1, at 1149.

13. *Id.*

14. Lee, *supra* note 9.

15. Jonathan Zittrain, *Law in a Networked World: Privacy 2.0+,* 2008 U. CHI. LEGAL. F. 65, 100 (2008).

Although users can control how much information they feel comfortable sharing on Facebook and adjust their privacy settings accordingly, it is almost certain that at least some of a user's "friends" will be able to see the content that he or she posts.[16] For example, hypothetically speaking, a user went to high school with Jane Doe; he searches for her on Facebook. If her privacy settings are such that she comes up in his search results, he can send her a message requesting that she accepts his friendship.[17] Then, the ball is in her court. She can unequivocally accept, granting him full access to all of the bits of information that she posts about herself, or, she can place him on a "limited profile," where she controls what information he can see, by limiting his access to only certain content.

Being a user's "friend," however, is not the only way that someone might gain access to a user's information. For example, a user might adjust his privacy settings so that everyone in his "Networks"[18] or all "Friends of Friends" can see certain posts.[19] For example, if a user posts an album with hundreds of pictures and allows everyone in his Stanford University network to see them, then the 50,587 members of that network (as of January 2010) would be able to see those pictures, regardless of whether they are "friends" with the user.

Methods of communication on social networking sites such as Facebook are also numerous. Users can send each other messages within the site, a feature that functions as Facebook's own version of emails. Users can also post messages on each other's walls to convey information that they wish to be more public.[20]

16. "Friend" connections are the primary way that Facebook users are linked. When users are "friends," they generally have access to each other's profiles and the information that they therefore post.

17. Users can adjust their privacy settings so that, at the most narrow, they are not searchable to anyone, even though their profile exists. At the opposite end of the spectrum, a user can be searchable to "Everyone," which means, anyone with a Facebook account.

18. A "Network" is a workplace or school that a user is or has been affiliated with. In order to join a school's network, for example, Facebook requires that a user verify his membership there with a valid school email address.

19. For a definition of "posts" *see* "Definitions," section 17 on Facebook's "Statements of Rights and Resposibilities," *available at* http://www.facebook.com/terms.php (last visited Jan. 25, 2010).

20. "[A] wall is a section in your profile where others can write messages to you or leave you gifts, which are icon-like small images. The wall is a public writing space so others who view your profile can see what has been written on your wall. Once you have received a wall message, you can respond directly back to the friend who left it using the "wall-to-wall" mode." *Definition of Facebook Wall*, WEBOPEDIA.COM, http://www.webopedia.com/TERM/F/Facebook_wall.html (last visited Jan. 25, 2010).

Because there are so many pieces of data floating around and there are so many different ways that users can be connected to one another, it is not surprising that Facebook and other social networking sites are rapidly becoming attractive places for the government to find pertinent information. The FBI, for example, has undercover agents in virtually every social network context.[21] Facebook explicitly warns that it "may disclose information pursuant to subpoenas, court orders, or other requests (including criminal and civil matters) if [they] have a good faith belief that the response is required by law."[22]

There have been several instances where the government—via local detectives, to prosecutors, to federal officials—has used information on social networking sites as "investigative, surveillance, and data collection tools."[23] John Carlin, Chief of Staff and Senior Counsel to the Director of the Federal Bureau of Investigation ("FBI"), delivered the keynote address at the Samuelson Conference where he revealed that the FBI has joined social networks and has used them in a variety of circumstances.[24]

When a Massachusetts man overdosed on heroin, local police detectives turned to his social networking pages (on both Facebook and MySpace) in order to get clues about the source of the drug and with whom the man might have been using.[25] The investigating detective explained, "People arrange to buy and sell drugs on Facebook . . . we'd be foolish not to use it as an investigative tool."[26]

In Cincinnati, the FBI was able to arrest seventy individuals who were associated with a violent gang called the "Taliband" by analyzing their connections on social networking sites.[27] These arrests

21. Paul Ohm, Lauren Gelman & Jack Bennett, Are You Really My Friend? The Law and Ethics of Covert or Deceptive Data-Gathering, address at Samuelson Conference, (Oct. 23, 2009), *available at* http://www.law.berkeley.edu/7458.htm.

22. *See How We Share Information* on Facebook's Privacy Policy, *available at* http://www.facebook.com/policy/php (last visited Jan. 25, 2010).

23. Elect. Frontier Found. v. Dept. of Defense, 2009 WL 4813489 (N.D.Cal. Dec. 1, 2009).

24. John Carlin, *Safety and Social Networks: the Challenge of Community Policing in a Virtual Neighborhood*, at Samuelson Conference, (Oct. 23, 2009), *available at* http://www.law.berkeley.edu/7458.htm.

25. Julie Masis, *Is This Lawman Your Facebook Friend? Increasingly, Investigators Use Social Networking Websites for Police Work*, THE BOS. GLOBE, Jan. 11, 2009, at 1 (NORTHWEST Reg).

26. *Id.* The article also reveals that in an informal survey of 14 departments in the area (Wilmington, Mass.), officials in half of them said that they use Facebook and MySpace when conducting their detective work.

27. Carlin, *supra* note 24.

resulted in a forty percent decrease in violent crimes in the area.[28] The FBI also used social networking data in a Colombia, Ohio gang shooting case, which was ironically instigated by discussions on social networks themselves.[29] By intercepting discussions about being "dissed" on MySpace, the FBI was able to establish a motive for a violent gang shooting.[30]

Facebook also provided the means for the government to apprehend a fugitive, Maxi Sopo, who allegedly stole more than $200,000 through a bank scam in Seattle.[31] While looking through Sopo's "friends" on Facebook, an Assistant United States Attorney ("AUSA") noticed that one of them was a former Department of Justice Attorney.[32] The AUSA contacted this former attorney, who looked through the pictures that Sopo had posted on his Facebook profile.[33] Sopo's pictures showed the fugitive partying in Cancun, where he was ultimately caught.[34]

Carlin also mentions that the government uses social networks to catch "tax deadbeats."[35] As he explains, there have been instances where individuals "claim poverty to the IRS," but their social networking profiles tell a different story—they brag about all of their wealth and assets through photographs and "vivid descriptions."[36]

An interesting dialogue at the Samuelson Conference between Paul Ohm, Lauren Gelman, and Supervisory Special FBI agent Jack Bennett shed light upon the law and ethics of what some might call "deceptive" data gathering.[37] Their discussion suggests that most states have not clearly defined when it is okay and when it is not okay to go undercover to gain information off of social networking sites.[38] Gelman does, however, consider that when a Facebook user changes his "network" so that he can gain access to information that is

28. *Id.*

29. *Id.*

30. *Id.* It should be noted that in his speech, Carlin did not explain the legal methods by which the FBI was able to intercept those discussions. It very well may be that the files were publicly available.

31. Chris Ayres, *The Fraud Suspect Who Was Asking to be Caught*, THE TIMES (London), Oct. 19, 2009, at 38.

32. Carlin, *supra* note 24.

33. *Id.*

34. *Id.*

35. *Id.*

36. *Id.*

37. Ohm, Gelman & Bennett, *supra* note 21.

38. *Id.*

available in a different network, that constitutes deception.[39] And Bennett admits that the FBI uses social networks for "ID takeovers" when they arrest a "bad guy."[40]

Both Gelman and Ohm think that there must be a new definition of a "reasonable expectation of privacy" in the new world of social networks. Ohm suggests that we "throw out *Katz*" and find something new.[41] But, Bennett offers a compelling counter-argument: that the whole idea behind social networking is to put information "out there for people to see" and therefore, it is "hard to believe" that there is an expectation of privacy if a user is "opening up his information for everyone to see."[42]

The government's use of social networking goes beyond criminal investigations and can involve matters of national security. Carlin warns that terrorist groups are using those sites to recruit members and spread ideologies.[43] For example, the Facebook group "Ahlus Sunnah wal Jama'ah" has reportedly recruited several students from British Universities and their group page contains links to literature such as *Jihad: a Ten Part Compilation,* which commands that all Muslims participate in violent jihad.[44] If extremist groups are truly infiltrating social networking sites, then the government has a legitimate interest in accessing data it is believes may threaten the United States. However, the government is unclear about to what extent it is privy to the abundant social networking data available.[45]

A member of the Facebook legal department explained that Facebook is committed to protecting its users' privacies at all costs.[46] The company has a process in place for responding to subpoenas.[47] According to Facebook, the California-based company applies the

39. *Id.*

40. *Id.* For example, the FBI will assume the "bad guy's" Facebook profile when he is arrested in order to gain access to other potentially incriminating information.

41. *See Katz v. United States*, 389 U.S. 347 (1967) (extending the Fourth Amendment to the government's electronic eavesdropping when a person has a reasonable expectation of privacy).

42. Ohm, Gelman & Bennett, *supra* note 21.

43. Carlin, *supra* note 24.

44. Danny Mendez, *Facebook and Terrorism: A Love Hate Relationship*, (Feb. 15, 2008). TECH.BLORGE.COM, http://tech.blorge.com/Structure:%20/2008/02/15/facebook-and-terrorism-a-love-hate-relationship-2/.

45. *See* FOIA, 5 U.S.C. § 552 (2010); *See also* EFF. v. Dept. of Defense, 2009 WL 4813489 (N.D.Cal. 2009).

46. Telephone interview with member of Facebook legal department, (Dec. 22, 2009) (transcript with author).

47. *Id.*

"strictest standards" when local sheriffs serve subpoenas for local information, but does not accept out-of-state subpoenas.[48] As explained in Facebook's Terms of Service, the company will provide information through valid legal process, which includes (as will be discussed later) what is statutorily required, and also in cases of imminent harm, such as kidnapping or matters of "absolute national security."[49]

Recognizing that its primary purpose is to serve as an identity service for people across the Internet, Facebook stresses that the site balances protecting its users' data with the countervailing interest of assisting law enforcement in accordance with existing statutes.[50] Experts in the field have argued that the Electronic Communications Privacy Act ("ECPA")[51] (discussed in detail in Part Three), which regulates the use of online data, is an antiquated statute.[52] Given the current state of the ECPA, and despite Facebook's best efforts to protect its users, it might be very difficult, from a legal standpoint, for providers like Facebook to fully protect its users' information from government access.[53]

III. Statutory and Legal Framework

The ECPA comprises the statutory framework that regulates the government's seizure and use of electronic data.[54] The ECPA gives the government access to both content and non-content data in stored wire or electronic communications. The statute "governs government access to stored wire and electronic communications in a 'facility' through which an electronic communication service is provided."[55] Sections 2703 and 2709 of the ECPA in particular have been the subject of the most relevant litigation about the legal issues surrounding access to social networking data.

48. *Id.*

49. *Id.*

50. *Id.*

51. See *infra* Part III.

52. James Aquilina, Executive Managing Director and Deputy General Counsel at Stroz Friedberg, *Does Overt Access to Social Networking Data Constitute Searching or Spying?*, address at Samuelson Conference, (Oct. 23, 2009), *available at* http://www.law.berkeley.edu/7458.htm; *see also, infra* note 52.

53. Aquilina, *supra* note 50.

54. Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2701–2711 (2010). The portions of the ECPA discussed in this note are commonly referred to as the "Stored Communications Act" ("SCA").

55. 18 U.S. NITA prec §2701.

Under the ECPA section 2703, if the contents of a wire or electronic communication have been in electronic storage or in an electronic communications system for one hundred and eighty days or less, a "governmental entity may require the disclosure . . . only pursuant to a warrant issued [pursuant to procedures under Federal or State law] . . ."[56] If, however, the contents of a wire or electronic communication have been in electronic storage in an electronic communications system for more than one hundred and eighty days, the government may obtain them either by a warrant (without notice to the subscriber or customer), by an administrative subpoena authorized by a federal or state statute or a federal or state grand jury or trial subpoena (with prior notice to the subscriber or customer), or a court order for disclosure.[57]

The ECPA, as amended and expanded by the USA Patriot Act, gives an electronic service provider or a remote computing service provider discretion to voluntarily disclose content and non-content information to the government.[58] If it is determined that the "provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency," he may divulge a record or other information pertaining to a subscriber to or customer of such service to a government entity.[59]

Section 2709 of the ECPA governs the procedure that allows the FBI to gain access to subscriber information or electronic communication transactional records if it is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities.[60] In these circumstances, the FBI may request (through national security demand letters, ("NSLs") the "name, address, length of service, and local and long distance toll billing records of a person," so long as the government's investigation of such person is not conducted solely on the basis of activities protected by the First Amendment.

Section 2709 also allows the FBI, in the event of national security, criminal, counterterrorism, or counterintelligence investigation, to prevent disclosure of such a request for information to any person.[61]

56. 18 U.S.C. §2703(a).
57. 18 U.S.C. §2703(b).
58. ECPA, 18 U.S.C. §§ 2701–2711 (2010).
59. 18 U.S.C. §2702(c)(4).
60. 18 U.S.C. §2709(b)(1).
61. 18 U.S.C. §2709(c)(1).

As will be further discussed, this so-called "gag" provision has been the subject of ongoing litigation.

When the government has attempted to gain access to both content and non-content information, litigation has implicated the ECPA as it relates to the Fourth Amendment. The Fourth Amendment of the United States Constitution protects citizens "against unreasonable searches and seizures."[62] Although there are cases that have dealt with the Fourth Amendment as it applies to electronic communications, conspicuously absent is legislation or case law that has made the leap to social networking data specifically.[63]

To date, the legislation that surrounds government access to electronic data, both content and non-content alike, focuses mainly upon email and Internet protocol ("IP") information. What is more, the laws grant the government access to information often with few obstacles.

The seminal case for applying the Fourth Amendment comes from *Katz v. United States*.[64] In *Katz*, the issue was whether the government should have been allowed to introduce evidence of petitioner's conversations that were "overheard by FBI agents who had attached an electronic listening and recording device to the outside of the public telephone booth from which he had placed his calls."[65] The court concluded that the "Fourth Amendment protects people, not places" and that the "[g]overnment's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied . . . and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[66]

Today, modern extensions of *Katz* that bear the most similarity to data on social networking sites are those that surround the constitutionality of section 2703 of the ECPA, and how it relates to the government's seizure of Internet communications, specifically email. The Supreme Court has yet to formally extend *Katz*'s Fourth

62. U.S. CONST. amend. IV.

63. There are cases, however, that deal with the identity of Internet chat room and message board users, but those center mostly on the applicability of the First Amendment and its protection of the users' identities, rather than the Fourth Amendment right to seize the information. *Sew eg.,* Doe v. 2TheMart.com, Inc., 140 F. Supp. 2d 1088 (W.D. Wash. 2001).

64. Joshua L. Simmons, Note, *Buying You: The Government's Use of Fourth Parties to Launder Data About "The People,"* COLUM. BUS. L. REV. 950, 960–61 (2009). *See also Katz v. United States*, 389 U.S. 347 (1967).

65. *Katz,* 389 U.S. at 348.

66. *Id.* at 351, 353.

Amendment protection to email, and Congress has yet to amend the ECPA "even as electronic communication technologies have been modified and improved."[67] The lower courts, however, seem to be pushing for a change.

One such case is *Warshak v. United States*[68] where an Ohio District Court "boldly" extended Fourth Amendment protection to email. This decision affirmed by the Sixth Circuit on December 14, 2010, holds that the government must have a search warrant before it can secretly seize and search emails stored by email service providers.[69] A closer examination of the case provides a useful insight into the debate over information privacy and issues that are arising under the ECPA as technology progresses at a rapid rate.

In *Warshak*, the government obtained two orders under the ECPA's section 2703(d) to search Steven Warshak's emails after Warshak's company, Berkeley Premium Nutraceuticals, Inc., became the target of an investigation into "mail and wire fraud, money laundering, and other federal offense[es]."[70] The magistrate judge granted the application under section 2703(d), which gave the government access to, among other things, the contents of emails that had been "accessed, viewed, or downloaded" or that were more than 181 days old.[71] After receiving notice of the orders about a year later, Warshak filed a declaratory judgment action seeking to invalidate section 2703(d) under the Fourth Amendment and moved for a preliminary injunction, "seeking to enjoin the government from conducting further *ex parte* e-mail searches."[72] The district court granted Warshak's injunction, reasoning that Warshak would likely succeed on his Fourth Amendment claim "because [I]nternet users have a reasonable expectation of privacy in e-mails . . ."[73]

After a lengthy subsequent history, the Sixth Circuit announced that electronic communication "deserved more protection than . . . ECPA provides,"[74] but later proceeded to vacate the opinion, ultimately arguing that Warshak's Fourth Amendment claim was not

67. Tamar R. Gubins, Note, *Warshak v. United States: The Katz for Electronic Communication*, 23 BERKELEY TECH L.J. 723, 744 (Annual Review, 2008).

68. Warshak v. United States, 532 F.3d 521 (6th Cir. 2008) ("*Warshak I*").

69. Gubins, *supra* note 66, at 727; *see also* United States v. Steven Warshak, 2010 U.S. App. LEXIS 25415, at *2 (6th Cir. 2010) ("*Warshak II*").

70. *Warshak I*, 532 F.3d at 523, 524 (internal quotations omitted).

71. *Id.*

72. *Id.* at 523.

73. *Id.* at 524–25.

74. Gubins *supra* note 66 at 725.

ripe for judicial resolution.[75] One reason the court gave was that "[t]he Supreme Court ha[d] been especially reluctant to invalidate statutes on their face under the Fourth Amendment."[76] In vacating the preliminary injunction and remanding the case to the district court to dismiss Warshak's constitutional claim, the Sixth Circuit held that Warshak "still retained the right to challenge the district court's resolution of his motion . . . through an appeal of his criminal conviction."[77]

Finally, in its December 14, 2010 opinion, the Sixth Circuit monumentally extended *Katz*'s Fourth Amendment protection to email.[78] The court reasoned:

> Since the advent of e-mail, the telephone call and the letter have waned in importance, and an explosion of Internet-based communication has taken place. People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button.[79]

When analogizing the situation in *Warshak* to the social networking world, it is difficult to know where exactly to extend the analysis. Facebook users, for example, can send messages to each other, which function like emails. However, would the information that a user posts to his profile be considered email communication? Perhaps the only way to assess what section of the ECPA applies is to determine how long the content had been on the site and whether it was "stored" for purposes of the statute.

For example, the Supreme Court has held that the Fourth Amendment's protection does not apply when an individual voluntarily discloses information to a third party.[80] In *United States v. Forrester* (where defendants were charged with offenses relating to an ecstasy-manufacturing laboratory), the Ninth Circuit relied primarily upon a Supreme Court surveillance case, *Smith v. Maryland,* which

75. *Warshak I*, 532 F.3d at 523.

76. *Id*. at 529.

77. *Id.* at 534.

78. *See Warshak II,* 532 F.3d 521 (6th Cir. 2008).

79. *Id.* at 31–32.

80. United States v. Forrester*,* 495 F.3d 1041, 1048 (9th Cir. 2007), (quoting Smith v. Maryland*,* 442 U.S. 735, 743–44 (1979)).

involved the constitutionality of pen registers.[81] Both defendants were convicted on all counts, and defendant Alba appealed, challenging the validity of the government's computer surveillance.[82]

The Ninth Circuit concluded that the government's surveillance was analogous to the use of a pen register as defined in *Smith v. Maryland* and therefore did not constitute a search for Fourth Amendment purposes.[83] Furthermore, the court concluded that "e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that these messages are sent and these IP addresses are accessed through the equipment of their Internet service provider and other third parties."[84]

As social networking sites continue to grow and be a principle means for people to form connections and share information, it is unsurprising that terrorist groups are also taking advantage of this online medium.[85] Therefore, the government's access to data involving issues of national security falls under the ECPA's section 2709, which has also been the subject of recent litigation.

Two cases present an illustration of the issues that have arisen as a result of the Patriot Act's expansion of the government's access to information through the ECPA and the difficulty that the lower courts are having in resolving the delicate balance between national security concerns, the ECPA's section 2709, and individual privacy.

In *Doe v. Ashcroft,* plaintiffs, who included the American Civil Liberties Union ("ACLU"), challenged the constitutionality of the ECPA's section 2709[86] broad subpoena power with regards to the FBI's issuance of NSLs.[87] In this case, the lead plaintiff (John Doe), was an Internet access firm that received an NSL.[88]

Section 2709 "bars all NSL recipients from ever disclosing that the FBI has issued an NSL."[89] The District Court concluded that 1) section 2709's nondisclosure provision violates the Fourth

81. *Id.* at 1043. A pen register is a device that records numbers dialed from a phone line.

82. *Id.*

83. *Id.* (quoting *Smith*, 442 U.S. 735, 745–46 (holding that the use of a pen register does not constitute a search for Fourth Amendment purposes)).

84. *Forrester*, 495 F.3d at 1049; (Internal citation omitted).

85. *See* Carlin, *supra* note 24.

86. 18 U.S.C. §2709. *See also supra* notes 46, 48.

87. Doe v. Ashcroft, 334 F.Supp.2d 471, 475 (S.D.N.Y 2004).

88. *Id.*

89. *Id.*

Amendment because "at least as currently applied, it effectively bars or substantially deters any judicial challenge to the propriety of the NSL request, and 2) "the permanent ban on disclosure contained in section 2709(c) . . . operates as an unconstitutional prior restraint on speech in violation of the First Amendment."[90]

A similar issue arose in *Doe v. Gonzalez*.[91] There, the plaintiff, a member of a library association, received an NSL requesting "information . . . associated with a 'specific Internet Protocol address.'"[92] The complaint alleged that the "gag imposed by section 2709(c) is an unlawful prior restraint on speech."[93]

The district court applied strict scrutiny and concluded that the permanent gag provision of the statute was not "narrowly drawn to serve the government's broadly claimed compelling interest of keeping investigations secret" and granted Doe's motion for a preliminary injunction.[94] A panel for the Second Circuit then issued an order staying the preliminary injunction to give the federal government an opportunity to file an expedited appeal.[95] Upon that panel's denial of the applicant's subsequent motion to vacate the stay, petitioners filed an emergency application to the Supreme Court.[96] Justice Ginsburg, writing for the Court, held that the applicants had not shown cause "so extraordinary as to justify [the] Court's intervention" while the action was pending in the Second Circuit.[97]

Although the government accesses social networking data through statutory means, it also does so by sidestepping them. While statutory mechanisms are in place for the official solicitation of data, as shown by the litigation surrounding sections 2703 and 2709, the government has used undercover identities and deceptive practices to gain access to social networking information-actions that are not necessarily illegal under current standards.[98]

In *Theofel v. Farey-Jones*, the Ninth Circuit considered "whether defendants violated electronic privacy and computer fraud statutes when they used a patently unlawful subpoena to gain access to e-mail

90. *Id. See also supra* notes 58, 60.

91. Doe v. Gonzalez, 546 U.S. 1301, 1302 (2005).

92. *Id.*

93. *Id.*

94. *Id.* at 1304–05 (internal citation omitted).

95. *Id.* at 1301–02.

96. *Id.* at 1302.

97. *Id.* at 1308.

98. *See supra* Part II (including an in-depth look at the government's use of undercover agents on social networking sites).

stored by plaintiff's Internet service provider."[99] Although the case involved private parties and not the government, the court provided some useful dicta on deception as it applies to the ECPA's section 2701. The court noted that the Stored Communications Act "protects individuals' privacy and proprietary interests" and "reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility."[100]

Although the court stated that a defendant is not liable for trespass if the plaintiff authorized his entry, it found that a police officer who "invited in a home, conceals a recording device for the media" is liable.[101] More specifically, the deceit must be a "substantial mistake . . . concerning the nature of the invasion or the extent of the harm."[102] The court then construed section 2701 in light of that analysis, holding that "permission to access a stored communication does not constitute valid authorization if it would not defeat a trespass claim in analogous circumstances."[103]

IV. Analysis and Proposal

As courts have struggled with the ECPA as it applies to the ongoing growth of technology, many have noted that the ECPA "provide[s] quite narrowly defined protections [and that] [t]hese limited provisions do not address the broad, ongoing changes in communications technologies."[104] The ACLU has also commented on the intersection between technology, liberty, and surveillance, arguing that the USA Patriot Act has "vastly expanded the FBI's authority to collect information about people it does *not* suspect of wrongdoing, including financial, credit and communications information, using NSLs . . ."[105] Michael Macleod-Ball, Acting Director of the ACLU Washington Legislative Office, argues, "[o]nce again, the FBI has been found to be using invasive 'counterterrorism' tools to collect

99. 341 F.3d 978, 981 (9th Cir. 2003), *amended* 359 F.3d 1066.

100. *Id.* at 982.

101. *Id.* at 982–83 (internal citations omitted).

102. *Id.* at 983 (internal citation omitted).

103. *Id.*

104. Gubins, *supra* note 66, at 740.

105. Press Release, American Civil Liberties Union, FBI Data Mining and Collection Programs Threaten Privacy of Innocent Americans (Sept. 24, 2009), *available at* http://www.aclu.org/pring/national-security_technology-and-liberty/fbi-data-mining-and-collection-programs-threaten-privacy-in (emphasis added).

personal information about innocent Americans . . . with little or no oversight."[106]

Thus, there are two main factors that necessitate a change. First, the ECPA has been expanded by the USA Patriot Act such that there are often few obstacles preventing the government from gaining access to data on social networking sites. Second, the rapid growth of the social networking world has changed the way people communicate across the Internet. Data sharing has gone from the age of email messages and IP address logs into a murky web of social networks and "wall posts." Therefore, the statutory and legal frameworks that currently exist are insufficient to encompass the way that contents are shared across the social network medium. Nor is this shift reflected in either the provisions of the ECPA or in the courts' applications of them.

For example, it is not entirely clear how section 2703 applies to a site like Facebook. There are probably messages and data that fall into the category of content that has been posted on the site for one hundred and eighty days or less, but what about the constant user behavior and interactions that comprise so much of what makes social networking sites unique?

The problem of what is content and non-content on social networking sites also confuses the issue. How would the non-content provisions of section 2703 that *Forrester* analogized to pen registers and applied to the "to/from" addresses in emails apply to behavior on Facebook? For example, the courts could extend that analogy to the social networking context by removing the expectation of privacy from data that a user makes public. For some users, that is merely who they are friends with on Facebook and the networks to which they belong, while for others it's virtually everything on their profiles.

Although there is a compelling argument under *Warshak II* that Facebook messages, like email, could likely be subject to a user's reasonable expectation of privacy, less clear is how far that reasonable expectation extends. Of course, any information that a user purposely makes open and publicly available to the millions on Facebook would be fair game. However, the problem lies in the murkier realm of semi-protected data—that is, data that a user only intends to share with those in a particular limited friend network. The photos and status updates that a user makes available to that limited friend network cannot be classified the same way as a private message intended between two people. However, a user's ability to

106. *Id.*

control how far the sharing of such data extends is a difficult issue unique to Facebook and the "network" setting, since that network could include every person in a large geographic region such as San Francisco, or a limited group of close friends.

Another problem with the ECPA is in the gag provision of section 2709 that is currently the subject of much debate. If social networks are quickly becoming a convenient place to facilitate terrorist communication, then sites like Facebook become an easy target for the government. If an NSL demands that Facebook hand over the profile information for a suspected terrorist involved in a matter of national security, it is likely that the government will also gain access to information that is not necessarily pertinent to the investigation. This is because the data on social networks is not as clearly defined or as compartmentalized as data in emails, for example.

As is evidenced by the current case law surrounding section 2703 and section 2709 specifically, these issues will only continue to present themselves in the social networking age. Although the case law as it currently stands extends primarily to email and ISP information, it seems that even there, the courts have been reluctant to make any Fourth Amendment extensions without statutory revisions from Congress.

There needs to be some sort of action from Congress, therefore, remodeling the ECPA to reflect the technological changes that have boomed in the past few years. There also needs to be a new *Katz*, as Ohm suggested, that defines the Fourth Amendment as it pertains to social networks. With that definition needs to come an explanation of what is considered "deception" in the social network medium. Unfortunately, a cop posing as a drug dealer on the streets to catch a criminal is not necessarily the same thing as an FBI agent who assumes a real person's online identity when that person is taken into custody.

The counter-argument—that people who post content should be aware of how visible it is to others—is a compelling one. In a culture so hooked on sharing information at rapid rates, people need to be aware that sometimes, what seems private is in fact not so. Regardless, while some of these individuals may be at fault for making their data widely known, those who have chosen to keep their online identities far more private will still be susceptible to government investigations that are currently not banned by either the ECPA or Supreme Court precedent.

V. Conclusion

While it remains unclear to what extent the government is actually using the data from social networks under the ECPA, the Samuelson Conference makes it abundantly clear that the government is obtaining the information. As forums continue to allow individuals to post content about themselves and communicate on a widespread level with others, courts are in need of greater guidance with respect to the government's search for online information.