**Cornell Journal of Law and Public Policy**

Volume 22
Issue 2 *Winter 2012*

Article 7

# Social Networking and the Fourth Amendment: Location Tracking on Facebook, Twitter, and Foursquare

Lisa A. Schmidt

Follow this and additional works at: http://scholarship.law.cornell.edu/cjlpp

 Part of the Law Commons

Recommended Citation
Schmidt, Lisa A. (2012) "Social Networking and the Fourth Amendment: Location Tracking on Facebook, Twitter, and Foursquare," *Cornell Journal of Law and Public Policy*: Vol. 22: Iss. 2, Article 7.
Available at: http://scholarship.law.cornell.edu/cjlpp/vol22/iss2/7

This Note is brought to you for free and open access by the Journals at Scholarship@Cornell Law: A Digital Repository. It has been accepted for inclusion in Cornell Journal of Law and Public Policy by an authorized administrator of Scholarship@Cornell Law: A Digital Repository. For more information, please contact jmp8@cornell.edu.

# NOTE

# SOCIAL NETWORKING AND THE FOURTH AMENDMENT: LOCATION TRACKING ON FACEBOOK, TWITTER, AND FOURSQUARE

*Lisa A. Schmidt**

*In the 2012 case* United States v. Jones, *Justice Samuel Alito asked whether the Fourth Amendment might extend any protection to new technology. Although the government may not track an individual through the use of Global Positioning System (GPS) services, the Supreme Court's past cases suggest that the same protection will not extend to new technologies like social networking. Popular social networking websites Facebook, Twitter, and Foursquare allow users to keep others aware of their location at all times, leading to the question of whether the government may track a user's location through social networking use. The author argues that past Fourth Amendment case law warns social networking users that the government may track location through tags and check-ins, and Internet users may not have the standing to raise a privacy claim for such tracking. The author concludes that Internet users must maintain their own privacy because the government may use any public information to track their locations.*



* J.D., Cornell Law School, 2013; B.A., Boston College, 2007. The utmost gratitude goes to my parents, the kindest people I know.

## INTRODUCTION: SOCIAL NETWORKS AND PRIVACY[1]

The Fourth Amendment to the United States Constitution states that the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause . . . ."[2] Recent Internet developments raise the question of whether this right extends to social networking. Even Justice Alito recognized the issue in his *United States v. Jones* concurrence, noting that social tools "will . . . shape the average person's expectations about the privacy of his or her daily movements."[3]

In the social networking context, can law enforcement use a photograph, check-in, or status update posted online to justify further search or

---

[1] The descriptions of social networking websites within this Note reflect the policies and format of the websites at the time of writing. The privacy policies of social networking websites are constantly evolving and may change at any time after the researching and writing of this Note.

[2] U.S. CONST. amend. IV.

[3] 132 S. Ct. 945, 963 (2012) (Alito, J., concurring) ("Similarly, phone-location-tracking services are offered as 'social' tools, allowing consumers to find (or to avoid) others who enroll in these services. The availability and use of these and other new devices will continue to shape the average person's expectations about the privacy of his or her daily movements.").

even arrest? Under current Fourth Amendment case law, most notably *Katz v. United States*,[4] the answer seems to be yes. Justice Harlan's concurring opinion in *Katz v. United States* has come to govern the standard for what qualifies as a search under the Fourth Amendment.[5] In short, the Fourth Amendment applies in situations where an individual has a reasonable expectation of privacy.[6] This standard cannot be satisfied in social networking. From news stories to privacy controls and even to user updates themselves, there may be no real protection from the authorities when one posts online.

This Note details applicable Fourth Amendment case law and concludes that all social networking users should be wary of the information they post online. Government officials may use public information to justify an arrest or conviction, and without Fourth Amendment protection, users may be subject to criminal liability based on personal photographs, location check-ins, or status updates posted on social networking websites.

The statistics on social networking are staggering. The most popular social networking website, Facebook, has become a worldwide phenomenon.[7] Facebook allows users to share photos, status updates, their location, and other media with their "friends."[8] Facebook alone has more than one billion users, and the average Facebook user shares ninety pieces of information each month.[9] Facebook sees over one million photographs uploaded every twenty minutes.[10] Additionally, more than six hundred million active users access Facebook through an application on their mobile phone, and many of these users stay logged into Facebook for extended periods of time, with the mobile phone application tracking their location.[11] Facebook states that it has seen over seventeen billion location-tagged posts, including check-ins to the user's current location.[12]

Twitter is a social networking website that allows users to share small status updates (under 140 characters) and photos with their "fol-

---

4 389 U.S. 347, 359 (1967).

5 *See id.* at 360 (Harlan, J., concurring).

6 *See id.*

7 *See generally* Dan Fletcher, *How Facebook Is Redefining Privacy*, TIME (May 20, 2010), http://www.time.com/time/magazine/article/0,9171,1990798,00.html.

8 *See id.*

9 *See One Billion Fact Sheet*, FACEBOOK, http://newsroom.fb.com/imagelibrary/downloadmedia.ashx?MediaDetailsID=4227&SizeId=-1 (last visited Oct. 19, 2012); Adam Ostrow, *What happens after your final status update?* CNN (Sept. 4, 2011), http://www.cnn.com/2011/OPINION/09/03/ostrow.status.final/index.html.

10 Aden Hepburn, *Facebook Statistics, Stats & Facts for 2011*, DIGITAL BUZZ BLOG (Jan. 18, 2011), http://www.digitalbuzzblog.com/facebook-statistics-stats-facts-2011/.

11 *See One Billion Fact Sheet*, *supra* note 9.

12 *Id.*

lowers."[13] Twitter status updates sometimes reflect the users' random thoughts, but users also post their locations or photos in their "tweets."[14] Twitter has over 100 million active users worldwide, and the website manages an average of 230 million tweets everyday.[15] While half of those 100 million users log into Twitter daily, some 40% of users do not share updates of their own, but instead merely view the tweets posted by others.[16]

Finally, Foursquare, a relatively new social networking platform, allows users to "check-in" to locations, providing real-time updates of the users' locations.[17] Foursquare currently has over 10 million users.[18] Foursquare is also accessible through a mobile phone application, allowing instantaneous sharing of information, but many users fail to consider the public exposure of their whereabouts.[19]

With so many social networking website users, there is a need to protect the information placed on those websites. For example, what happens to users who do not properly manage their use of these websites? Is there any protection against the police using that information, in the form of photos, check-ins, or tags, to justify a search or even an arrest? Do users face police action based on their online postings? The Supreme Court has yet to weigh in on the Fourth Amendment's relationship with social networking, but as technology continues to advance and as Justice Alito noted in *United States v. Jones*,[20] the Court will have to examine these issues soon.

This Note focuses on the privacy implications of social networking activity in the context of location tracking. Facebook, Twitter, and Foursquare are all capable of tracking users' locations while they are logged into the website, and the Fourth Amendment may not apply to this type of location tracking. This Note also discusses the Fourth Amendment

---

13 *About Twitter*, TWITTER, https://twitter.com/about (last visited Oct. 19, 2012).

14 *Id.*

15 Bianca Bosker, *Twitter Finally Shares Key Stats: 40 Percent of Active Users Are Lurkers*, HUFFINGTON POST (Sept. 8, 2011, 2:51 PM), http://www.huffingtonpost.com/2011/09/08/twitter-stats_n_954121.html.

16 *Id.*

17 Bianca Bosker, *Foursquare Celebrates 10 Million Users, Reveals New Stats*, HUFFINGTON POST (June 20, 2011, 6:04 PM), http://www.huffingtonpost.com/2011/06/20/foursquare-10-million-users-stats_n_880772.html.

18 *Id.*

19 *See Some Notes on Foursquare and Location Sharing*, FOURSQUARE LABS, INC., http://blog.foursquare.com/2010/08/17/967910179/ (last visited Oct. 19, 2012).

20 *See* United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring) (noting that "phone-location-tracking services are offered as 'social' tools, allowing consumers to find (or to avoid) others who enroll in these services. The availability and use of these and other new devices will continue to shape the average person's expectations about the privacy of his or her daily movements.").

case law detailing the reasonable expectation of privacy standard[21] and concludes that any media placed on social networking websites—including location check-ins—may be without Fourth Amendment protection, because, in the words of the *Katz* opinion, the social networking users knowingly exposed that information to the public.[22] Thus, Government officials may use any information posted on these websites to justify an arrest or as evidence in a case against a suspect. This Note details the users' need to remain aware of publicly viewable information on social networking websites, from photographs and status updates to location check-ins.

Part I of this Note discusses the *Katz* reasonable expectation of privacy standard. Part II details Fourth Amendment doctrine in the context of location tracking, including considerations of plain view movements and the use of Global Positioning System (GPS) trackers. Part III discusses various implications of the Fourth Amendment in social networking, including consent and "opting in" to the privacy rules of Facebook, Twitter, and Foursquare. This Part also addresses recent developments in several cases implicating Fourth Amendment protection in social networking use. Part IV discusses some of the foremost Supreme Court Fourth Amendment cases, specifically those involving new technology and plain view surveillance. Part V focuses on the Supreme Court's development of the "pretend friend" doctrine. Lastly, Part VI examines additional considerations in a social networking search analysis, including youth privacy and suppression claims.

## I. *KATZ V. UNITED STATES* AND THE REASONABLE EXPECTATION OF PRIVACY TEST

The leading case governing Fourth Amendment searches remains *Katz v. United States*.[23] In *Katz*, Justice Harlan argued in his concurrence that Fourth Amendment violations must be decided under a reasonable expectation of privacy standard.[24] In this case, the defendant used a public pay phone to place illegal gambling wagers.[25] The FBI had attached an electronic device to the phone booth to listen to Katz's call, and the officers used the information that they gathered while listening to the call to justify Katz's arrest and conviction.[26] Katz appealed his conviction, claiming that the use of the electronic device constituted a search in violation of the Fourth Amendment.[27] The Supreme Court agreed

21 *See* Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).
22 *See id.*
23 *Id.* at 359.
24 *Id.* at 360.
25 *See id.* at 348.
26 *See id.*
27 *Id.* at 350.

with Katz, stating that the wiretapping constituted a search because it violated Katz's reasonable expectation that his conversation would not be broadcast to the world regardless of the lawfulness of Katz's actions.[28]

As the *Katz* Court stated, "Virtually every governmental action interferes with personal privacy to some degree. The question in each case is whether that interference violates a command of the United States Constitution."[29] The Fourth Amendment right against unlawful searches and seizures governs the inquiry.[30] Writing for the majority, Justice Stewart argued that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[31]

Because social networking websites are still in their infancy, the Court has yet not narrowed the definition of "knowingly exposed" for application to social networking website activity. However, these websites have become one of the most common modes of communication, and it seems inevitable that this issue will soon reach the Court.[32] Because of the privacy guidelines disclosed on each social networking website, location check-ins may be considered knowingly exposed to the public; to join a social network, the user must respond to the standard privacy policy and accept the terms-of-use agreement.[33] A user may argue that her social networking use is not aimed toward the public dissemination of personal information, but that user posts with the hope that the community will see the information. A user posts with the understanding that the information put on social networking websites will be broadcast to the world and, thus, knowingly exposed. Therefore, under the *Katz* framework, it seems that the average social networking website user will not receive the benefit of the Fourth Amendment's protections for her online social networking activity.

Under *Katz*, even if the information is knowingly exposed, what a defendant "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[34] In a public phone booth, for example, an individual "is surely entitled to assume that the words he

---

28 *Id.* at 356–57.

29 *Id.* at 350 n. 5.

30 *Id.*

31 *Id.* at 351.

32 *See* United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring) (noting that "phone-location-tracking services are offered as 'social' tools, allowing consumers to find (or to avoid) others who enroll in these services. The availability and use of these and other new devices will continue to shape the average person's expectations about the privacy of his or her daily movements.").

33 *See infra* Part III.

34 *Katz*, 389 U.S. at 351.

utters into the mouthpiece will not be broadcast to the world."[35] However, many users communicate via social networking precisely for the purpose of broadcasting information to the world, or at least to the insular social world of their friend network.[36] While some web users have already suffered criminal sanctions for actions described in social networking "brags,"[37] even more users likely remain unaware of the legal consequences of what they post online.

## II. LOCATION TRACKING AND THE FOURTH AMENDMENT

### A. United States v. Karo: *Tracking Movement*

Does the Fourth Amendment protect any form of location tracking? The Supreme Court looked at this question in *United States v. Karo*.[38] In *Karo*, the police used a beeper to track the movement of a can of ether inside the defendant's house.[39] The Court stated that the defendant had a reasonable expectation of privacy in his home and that, because the officers could not have seen what was happening inside the house, the beeper gave the Government sensitive information from a constitutionally protected area.[40] Because the Government obtained the information through means beyond their own sensory perception, the use of the beeper constituted a search.[41] However, the Court modified this doctrine in *United States v. Knotts*.[42]

### B. United States v. Knotts: *Location Tracking in Plain View*

*Smith v. Maryland*[43] restated the following test for reasonableness under *Katz*: "application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action."[44] Under this test, a court must answer two questions. First, it must consider "whether the individual, by his conduct, has 'exhibited an actual (subjective) expectation of privacy,'"[45] specifically,

---

35 *Id.* at 352.

36 *See generally Social Networking's Good and Bad Impacts on Kids*, AM. PSYCHOLOGICAL ASSOC. (Aug. 6, 2011), http://www.apa.org/news/press/releases/2011/08/social-kids.aspx (noting teenagers' narcissistic tendencies in Facebook posting).

37 *See, e.g.*, Kelly Burgess, *Facebook Bragging About Poaching Leads to Charges Against Man*, L.A. TIMES (May 27, 2011, 10:27 AM), http://latimesblogs.latimes.com/outposts/2011/05/facebook-bragging-leads-to-felony-poaching-arrest.html.

38 478 U.S. 705, 707 (1984).

39 *Id.* at 707.

40 *Id.* at 715.

41 *Id.*

42 460 U.S. 276 (1983).

43 442 U.S. 735 (1979).

44 *Id.* at 740 (citations omitted).

45 *Id.* (quoting Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

if "'he seeks to preserve [something] as private.'"[46] Second, that court must consider "whether the individual's subjective expectation of privacy is 'one that society is prepared to recognize as 'reasonable.'"[47] Specifically, was the expectation justifiable "under the circumstances"?[48]

In *United States v. Knotts*,[49] Government officials tracked the movement of the defendant's car using a beeper device placed inside a container of chloroform.[50] The car carrying the container travelled on "public thoroughfares where both its occupants and its contents [were] in plain view."[51] The Court rejected the defendant's Fourth Amendment claim, holding that no search had taken place because anyone could have seen the car's public movements, so the use of the beeper was therefore irrelevant.[52] The Court held that if the car was in public view, there was no reasonable expectation of privacy.[53] Accordingly, "[n]othing in the Fourth Amendment prohibited the police from augmenting the sensory facilities bestowed upon them at birth with such enhancement as science and technology."[54] In other words, the Court was prepared to endorse a plain view exception[55] to the search and warrant requirements of the Fourth Amendment, a concept that can easily extend to information displayed online, from locations such as in *Knotts* to photographs detailing criminal actions.

### C. United States v. Jones: *The Fourth Amendment and GPS Tracking*

In the 2012 case *United States v. Jones*,[56] the Supreme Court held that the use of a GPS tracker to monitor a car's movement constitutes a search under the Fourth Amendment.[57] In *Jones*, District of Columbia police suspected the defendant of trafficking drugs and hoped to obtain information about Jones's whereabouts to determine his role in a conspiracy to possess and distribute cocaine.[58] Officers attached a GPS tracker

---

46 *Id.* (quoting *Katz*, 389 U.S. at 351).

47 *Id.* (quoting *Katz*, 389 U.S. at 361).

48 *Id.* (quoting *Katz*, 389 U.S. at 355 n. 5).

49 460 U.S. 276, 277 (1983).

50 *Id.*

51 *Id.* at 281 (quoting Cardwell v. Lewis, 417 U.S. 583 (1974) (plurality opinion)).

52 *Id.* at 285.

53 *Id.* at 281.

54 *Id* at 282.

55 Under the plain view exception to the Fourth Amendment, officers may seize evidence found in plain view if they are engaged in legitimate police activity. *See* Horton v. California, 496 U.S. 128, 142 (1990). Similarly, if an officer hopes to obtain a warrant, his observations of plain view evidence may provide the basis for probable cause to search. *See* Steele v. United States, 267 U.S. 498, 504–05 (1925).

56 132 S. Ct. 945 (2012).

57 *See id.* at 951–52.

58 *See id.* at 948. The District of Columbia police obtained a warrant to attach a GPS tracker to Jones's car, but the tracker was attached in Maryland rather than the District of

to Jones's car and received more than 2,000 pages of data from the tracker that ultimately placed Jones at the conspirators' "stash house," which contained $850,000 in cash, ninety-seven kilograms of cocaine, and one kilogram of cocaine base.[59] The Government argued that the defendant had no reasonable expectation of privacy in his plain view movement under *Knotts*, and, therefore, the tracking did not implicate the Fourth Amendment.[60] The Court, however, held that the use of a GPS tracker to track a car's movement was a search under the Fourth Amendment.[61]

Justice Sotomayor's concurring opinion emphasized the physical intrusion into Jones's property,[62] while Justice Alito concurred under the *Katz* reasonable expectation of privacy test.[63] Justice Alito specifically noted the growing use of tracking through mobile devices, stating that tracking through "'social' tools" on phones can shape expectations of privacy.[64] While the Government may not attach a GPS tracker to one's "effects" under the Fourth Amendment, *Jones* likely does not preclude tracking movement through social networking websites. First, the *Jones* Court partly rested its holding on the physical intrusion into private property.[65] If police choose to track an individual's movement through social networking website activity, a court could reasonably conclude that there is no physical intrusion because the movement information is publicly available. Second, social networking activity may not be private property, in part because the user opts in to using the website and accepts the privacy agreements imposed by the social networking company.[66]

However, the Court noted that physical intrusion is not the only relevant inquiry; rather, the Fourth Amendment commands a combination of the *Katz* reasonable expectation of privacy test with a "common-law trespassory test."[67] Social networking tracking would likely pass both parts of this test because, here, there is neither a reasonable expecta-

---

Columbia. Thus, the Government was forced to concede that it did not comply with the warrant but argued that no warrant was required under the Fourth Amendment. *See id.*

59 *Id.* at 948–49.

60 *See id.* at 950.

61 *Id.* at 951–52.

62 *See id.* at 954–55 (Sotomayor, J., concurring).

63 *See id.* at 957–58 (Alito, J., concurring).

64 *See id.* at 963 ("Similarly, phone-location-tracking services are offered as 'social' tools, allowing consumers to find (or to avoid) others who enroll in these services. The availability and use of these and other new devices will continue to shape the average person's expectations about the privacy of his or her daily movements.").

65 *See id.* at 949.

66 *See* discussion on privacy policy, *infra* Part III, noting that social networking companies gain control over information posted on their websites.

67 *Jones*, 132 S. Ct. at 952 ("[A]s we have discussed, the Katz reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.") (emphasis in original).

tion of privacy under *Katz*, nor is there physical trespass. Additionally, the inquiry could turn on the Internet's status as a "protected area" under the Fourth Amendment.[68] While it is only one part of a Fourth Amendment test, and it may not decide Fourth Amendment reasonableness, a court could conclude that social networking websites are not protected areas, and, thus, a user has no reasonable expectation of privacy.

## III. SOCIAL NETWORKING AND FOURTH AMENDMENT IMPLICATIONS

### A. *Social Networking and Consent*

As discussed in Part I *supra*, the average social networking website user may have no real expectation of privacy regarding the information that she shares on social networking websites. There is, however, another consideration in the Fourth Amendment context. Even if the Court were to hold that social networking websites are subject to Fourth Amendment protection, much of the user information viewable by law enforcement on those websites may instead fall within the consent search framework. That is, while the violation of an individual's reasonable expectation of privacy would normally require a warrant, an individual's consent justifies the search without that warrant.[69] Thus, even if the discovery and use of the evidence constitutes a search, social networking website users may have consented to law enforcement officials' viewing their personal information.

Although the line between consensual and non-consensual searches may be unclear,[70] the Court justifies this uncertainty because of the "overlap" between the two considerations. In a consent search, a person willingly gives up the right to privacy based on some action on her part, usually by verbally agreeing to the search.[71] In the social networking context, therefore, the user's actions and acceptance of the website's privacy policy may be considered a general consent to a search. The privacy policies detailed in the following section further discuss the user's consent to the website's use of that user's information.

### B. *Privacy Rules*

Facebook's *Statement of Rights and Responsibilities* acts as the user's guidelines to privacy protections:

> You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings. In addition:

---

68 *See id.* at 953.

69 *See* Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 148 (2002).

70 *See id.*

71 *See id.*

> 1. For content that is covered by intellectual property rights, like photos and videos (IP content), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it.[72]

Twitter's privacy policy governs the user's status updates:

> Our Services are primarily designed to help you share information with the world. Most of the information you provide us is information you are asking us to make public. This includes not only the messages you Tweet and the metadata provided with Tweets, such as when you Tweeted, but also the lists you create, the people you follow, the Tweets you mark as favorites or Retweet and many other bits of information that result from your use of the Services. Our default is almost always to make the information you provide public for as long as you do not delete it from Twitter, but we generally give you settings to make the information more private if you want. Your public information is broadly and instantly disseminated. For instance, your public user profile information and public Tweets may be searchable by search engines and are immediately delivered via SMS and our APIs to a wide range of users and services, with one example being the United States Library of Congress, which archives Tweets for historical purposes. When you share information or content like photos, videos, and links via the Services, you should think carefully about what you are making public.[73]

Foursquare's privacy policy warns of the dangers of making information public to friends and others:

> Your "friends" can see the location and time of each of your check-ins, first name and last initial, email, phone number, photo, hometown, mayorships and badges, links

---

72 *Statement of Rights and Responsibilities*, FACEBOOK, http://www.facebook.com/legal/terms (last visited Sept. 7, 2012).

73 *Privacy Policy*, TWITTER, https://twitter.com/privacy (last visited Sept. 7, 2012).

> to your Twitter and Facebook accounts (if you have connected those accounts to your foursquare account), a list of your friends, Tips you write, and items on your To-Do list. . . . Individuals reading this information may use it or disclose it to other individuals or entities without our control and without your knowledge. We therefore urge you to think carefully about including any specific information you may deem private in Shouts or To Dos or other content (location or otherwise) that you create in the Service.[74]

### C. *Privacy Policies and Reasonable Expectations*

In *Katz v. United States,* Justice Harlan argued in his concurrence that "electronic as well as physical intrusion into a place [where a person has a constitutionally protected reasonable expectation of privacy] may constitute a violation of the Fourth Amendment."[75] This suggests that Internet use may be afforded some Fourth Amendment protection after all. Nevertheless, it may be difficult to draw the line between public and private electronic information on social networking websites. As Justice Black notes in his dissent in *Katz*, the Court may find it improper to extend Fourth Amendment protection merely "to bring [the law] into harmony with the times."[76] The privacy policies detailed above not only admit that much information may become public, but the websites themselves warn users against posting information that they may wish to keep private. Considering the language of these policies, it is difficult to accept that users do not knowingly expose this information online and that they maintain some expectation of privacy.

### D. *Recent Developments in Social Networking Use*

Aside from the tags that users apply to their photographs, locations, and status updates, Facebook and other social networking websites raise another issue—the use of "cookies" that track the user's web use outside of the social network. Specifically, if the user stays logged into a social networking website, the companies can track the websites viewed by the user and the locations from which those websites were accessed.[77] Many Facebook users keep their computer constantly logged into the website for reasons of convenience but most of those users are unaware that

---

74 *Privacy Policy*, FOURSQUARE LABS, INC., https://foursquare.com/legal/privacy (last visited Sept. 7, 2012).

75 Katz v. United States, 389 U.S. 347, 360 (Harlan, J., concurring).

76 *Id.* at 364 (Black, J., dissenting).

77 Class Action Complaint, Davis v. Facebook, Inc., No. 5:11-c-v-04834, at 2 (N.D. Cal. Sept. 30, 2011).

Facebook may be tracking their web use.[78] In September 2011, Facebook admitted that "it has installed the cookies on users' computers that track the internet [sic] activity of users *even after they have logged off of Facebook*."[79] Additional lawsuits were filed in Kansas over cookies and tracking.[80] Aside from the location tracking on computers, many users keep their smartphones constantly logged into the Facebook website.[81] The Supreme Court may be reluctant to endorse GPS-tracking,[82] but these websites are able to track user locations through the social networking website's mobile phone application.[83] Thus, while the computer tracking use is enough to heighten privacy concerns, users must also consider the reasonableness of their expectation of privacy on their mobile phones because at any time Government officials may use these applications to track a suspect's whereabouts without probable cause or a warrant.

While the privacy concerns are vast and complicated, there is hope for the ordinary user. That hope comes from what may be an unlikely place—lawmakers. Recently, United States senators John McCain and John Kerry, with the support of the Department of Commerce, introduced a bill proposing a "privacy bill of rights" for Internet users.[84] Congress is still considering this proposal, but, in the meantime, federal investigators continue to use social networking websites to their benefit. For example, in recent years, Government officials have obtained warrants for photographs, e-mail addresses, and friends lists to determine possible accomplices.[85] They have also used GPS locations to disprove alibis.[86]

Even with the potential protection of a statute, the average social networking website user may not actually be concerned about her privacy rights. Facebook creator Mark Zuckerberg, arguably the most

---

78 *See* Emil Protalinski, *Facebook Tracks You Online Even After You Log Out*, ZDNET (Sept. 25, 2011, 7:59 AM), http://www.zdnet.com/blog/facebook/facebook-tracks-you-online-even-after-you-log-out/4034. *But see* Emil Protalinski, *Facebook Denies Cookie Tracking Allegations*, ZDNET (Sept. 25, 2011, 4:25 PM), http://www.zdnet.com/blog/facebook/facebook-denies-cookie-tracking-allegations/4044 (Facebook denied tracking users after users logged out and asserted that they tracked user activity for Internet safety purposes).

79 Class Action Complaint, *supra* note 76 (emphasis in original).

80 *See* Rosanna Hegeman, *Man Sues Facebook Over Privacy Issues*, MSNBC.COM (Oct. 6, 2011, 6:40 PM), http://www.msnbc.msn.com/id/44809232/ns/technology_and_science-security/t/man-sues-facebook-over-privacy-issues/#.Tx4ZDZhA594.

81 *See One Billion Fact Sheet*, *supra* note 9.

82 *See* discussion *supra* Part II.C.

83 *See One Billion Fact Sheet*, *supra* note 9.

84 *See* Laura Vik, *Facebook and the Fourth Amendment*, BILL OF RIGHTS INSTITUTE BLOG (May 3, 2011), http://blog.billofrightsinstitute.org/2011/05/facebook-and-the-fourth-amendment/.

85 *See id.*

86 *See id.*

prominent figure in the social networking world, recently expressed the view that Facebook users do not care about their privacy.[87] After an unforeseen privacy breach on the Facebook website, Zuckerberg responded to the problem, stating:

> . . . [I]n the last 5 or 6 years, blogging has taken off in a huge way and all these different services that have people sharing all this information. People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that's evolved over time.[88]

Meanwhile, social networking website users may soon become more aware of the legal ramifications of the information they post online. Recently, Internet commentators have claimed that the use of social networking websites may enable social media companies to give the information users provide to a third party, including law enforcement officials.[89] As a result, social networking website users may wonder whether the Fourth Amendment protects them. This Note argues that the answer is probably no because the police will likely not be required to obtain a warrant to look at the publicly available information on these websites.

## IV. A BRIEF HISTORY OF FOURTH AMENDMENT DOCTRINE

### A. Ontario v. Quon: *The Fourth Amendment and New Technology*

In City of Ontario v. Quon,[90] the Supreme Court addressed a Government search implicating a new technology: a pager.[91] In Quon, the Government employer suspected inappropriate communication on the part of the defendant employee, and so it obtained transcripts of the defendant's text messages sent using a Government-issued pager.[92] The privacy policy considered in *Quon* stated that "the City 'reserves the right to monitor and log all network activity including e-mail and Internet use, with or without notice. Users should have no expectation of

---

87 *See* Helen A.S. Popkin, *Privacy Is Dead on Facebook. Get Over It.*, MSNBC.COM (Jan. 13, 2010, 8:56 AM), http://www.msnbc.msn.com/id/34825225/ns/technology_and_science-tech_and_gadgets/t/privacy-dead-facebook-get-over-it/#.TxxcHJhA594.

88 *Id.* (omission in original).

89 *See generally* Robert Charette, *Do Facebook Users Forfeit Their 4th Amendment Protections?*, IEEE SPECTRUM (Feb. 2010), http://spectrum.ieee.org/riskfactor/telecom/internet/do-facebook-users-forfeit-their-4th-amendment-protections#.

90 130 S. Ct. 2619 (2010).

91 *See id.* at 2624.

92 *See id.*

privacy or confidentiality when using these resources.'"[93] As the Court stated in *Quon*, the Fourth Amendment "'guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government,' without regard to whether the government actor is investigating crime or performing another function."[94] This case raised the question of what governmental action is arbitrary. Government officials may not look at tracking information aside from investigation into a crime,[95] but does the user still maintain that privacy and dignity in location? The issue remains open, and further application of this principle could change because of the constant evolution of new technology.

In *Quon,* the Court noted that "[c]ell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification."[96] This is especially relevant now, with mobile phones becoming even more easily accessible.[97] Internet use on these phones continues to alter the factors the courts must consider. The changing role of technology and communication implies the need for a reevaluation of policy and a continuing vigilance on the part of social networking users.[98]

### *B.* Florida v. Riley*: Plain View Surveillance*

In the 1989 case *Florida v. Riley*,[99] the Supreme Court considered the issue of police surveillance in the Fourth Amendment context.[100] In that case, a sheriff conducted surveillance from a helicopter after receiving an anonymous tip that the suspect, Riley, was growing drugs in a greenhouse in his backyard.[101] From an altitude of four hundred feet, the

---

93 *Id.* at 2625 (quoting Ontario's "Computer, Usage, Internet and E-Mail Policy").

94 *Id.* at 2627 (quoting Skinner v. Ry. Labor Execs. Assoc., 489 U.S. 602, 613–14 (1989)).

95 *See* Heather Kelly, *Police Embrace Social Media as Crime-Fighting Tool*, CNN (Aug. 30, 2012, 5:23 PM), http://www.cnn.com/2012/08/30/tech/social-media/fighting-crime-social-media/index.html; *see also* United States v. Meregildo, No. 11 Cr. 576 (WPH), 2012 U.S. Dist. LEXIS 115085, at *1 (S.D.N.Y. Aug. 10, 2012) ("When a social media user disseminates his postings and information to the public, they are not protected by the Fourth Amendment" (citing United States v. Katz, 389 U.S. 347, 351 (1967))).

96 Quon, 130 S. Ct. at 2630.

97 *See ITU Releases Latest Global Technology Development Figures*, INT'L TELECOMMC'N UNION (Oct. 11, 2012), http://www.itu.int/net/pressoffice/press_releases/2012/70.aspx ("Mobile-cellular subscriptions registered continuous double-digit growth in developing country markets, for a global total of six billion mobile subscriptions by end 2011.").

98 *See supra* note 64 and accompanying text (noting Justice Alito's recognition of tracking through social tools on mobile devices).

99 488 U.S. 445 (1989).

100 *See id.* at 447–48.

101 *See id.* at 448.

officer discovered the drugs without obtaining a search warrant.[102] Riley argued that the search was illegal without a warrant and that any information gained through this search of the interior of his residential backyard greenhouse should have been suppressed.[103] In a 5-4 decision, Justice White held for the Court that the action was not a search, and, therefore, the officer was not required to obtain a warrant under the Fourth Amendment.[104] According to the Court, flying at such an altitude was not contrary to any law, so any member of the public also could have potentially flown that close to Riley's greenhouse and observed his drug operation.[105] The Court noted, however, that if flying at that altitude had been against the law, the Government's actions could have constituted an illegal search.[106]

Thus, this case highlighted the notion of plain view and the issue raised in *Katz* of what information is knowingly exposed to the public. Applied to social media, could photographs or locations on social networking websites be considered plain view with no need for a warrant? While the social networking websites have privacy policies and terms of use as detailed in Part III.B *supra*, a future Court ruling may depend on the difference, or lack thereof, between public and private profiles.

## V. THE EXPECTATION OF PRIVACY IN FRIENDS AND RELATIONSHIPS: SOCIAL NETWORKING AND THE PRETEND FRIEND DOCTRINE

### A. *Informants and the Fourth Amendment*

#### 1. *Hoffa v. United States*: Misplaced Trust in Friends

How can ordinary human relationships and interactions color the Fourth Amendment context? The Supreme Court addressed this question in *Hoffa v. United States*.[107] In *Hoffa*, an informant obtained incriminating statements from mobster Jimmy Hoffa for use against him in a witness tampering prosecution.[108] The Court held that the use of an informant did not violate the Fourth Amendment because the defendant voluntarily gave incriminating information during an ordinary conversation.[109] According to the Court, "The Fourth Amendment can certainly be violated by guileful as well as by forcible intrusions into a constitu-

---

102 *See id.*
103 *Id.* at 447–48.
104 *Id.* at 450.
105 *Id.* at 451.
106 *Id.*
107 385 U.S. 293 (1966).
108 *See id.* at 294–95.
109 *See id.* at 303.

tionally protected area."[110] However, the Court held that even if the means are deceitful, Government officials are free to start a relationship with a suspect in the hope of receiving incriminating information.[111] The Court noted that no Justice "has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."[112] Thus, while the use of informants is deceptive, the Court held that "the [Government's] use of secret informers is not per se unconstitutional."[113]

### 2. *United States v. White*: Misplaced Trust and Technology

The Fourth Amendment also does not protect a wrongdoer's mistaken belief that a person to whom he voluntarily confides his wrongdoing will not reveal it. In *United States v. White*,[114] the Supreme Court ruled that a defendant has no reasonable expectation of privacy in the details of his conversation with an informant wearing a recording device.[115] The *White* Court found that those who choose to interact with and invest confidence in a person assume the risk of misplacing that confidence.[116] Therefore, under *White*, there is no reasonable expectation of privacy in one's friends, and individuals assume the risk that such conversations might be recorded.[117]

In dissent, Justice Harlan argued that the Court's holding undermined the sense of security innocent people have in interacting with others in a free society.[118] Police may use informants, but when recording devices are involved, the considerations are different.[119] Arguably, the Court's holding allows the Government to introduce an element that does not naturally exist in ordinary human interaction, thereby forcing citizens to question their relationships.[120] Therefore, Harlan argued, the government-issued friend is closer to the recording device used in *Katz* than it is to the ordinary friendship.[121]

---

110 *Id.* at 301.

111 *See id.* at 303.

112 *Id.* at 302.

113 *Id.* at 311.

114 401 U.S. 745 (1971).

115 *See id.* at 752.

116 *See id.*

117 *Id.*

118 *Id.* at 787 (Harlan, J., dissenting).

119 *See id.* at 772.

120 *See id.* at 787; Colb, *supra* note 69, at 143.

121 *See* Colb, *supra* note 69, at 143.

### *B. The Pretend Friend Doctrine*

Many of the recent Fourth Amendment decisions depend on the need for reliable evidence.[122] The Supreme Court is sometimes reluctant to recognize more Fourth Amendment violations because such violations lead to the suppression of valuable evidence, allowing a criminal to potentially go free.[123] Specifically, the Court has embraced the use of "false friends"[124] or "pretend friends"[125] to intercept information for use as evidence.

The Supreme Court has held that Government officials are free to act as pretend friends in an effort to gain the trust of a suspect in the hopes of eventually hearing incriminating information to use as evidence against that suspect.[126] Pretending to be a friend and ultimately betraying that purported friendship is not a criminal act.[127] In *Katz*, both parties, Katz and his listener, reasonably believed that the conversation was private and would not be intercepted.[128] However, in *White* and *Hoffa*, the suspect suffered no violation of privacy because one party to the conversation was a traitor that had no expectation of privacy and simply succeeded in obtaining incriminating evidence.[129] The differing outcomes of *Katz* and the various informant cases suggest that the Court expects a certain amount of betrayal and deception in friendships, either in the pretend friend cases or normal everyday interactions between real friends.[130]

Social networking website users naturally have similar expectations regarding friendship and privacy as those addressed in the pretend friend cases. This highlights a few considerations in the use of social networking websites. First, information on websites like Facebook, Twitter, and Foursquare may be public if the user does not set the privacy settings to display information only to those whom the user has confirmed as a "friend," raising various consent-to-search arguments. Secondly, a user may unknowingly confirm a pretend friend. Specifically, the user may allow an informant to view his or her private information on the social networking website under the assumption that the other user is a legitimate, regular user who has no investigative interest in the information posted but rather just wants to expand a social network and meet new

---

122 *See id.* at 121.

123 *See id.*

124 *See* Bernard W. Bell, *Secrets and Lies: News Media and Law Enforcement Use of Deception as an Investigative Tool*, 60 U. PITT. L. REV. 745, 800 (1999).

125 *See* Colb, *supra* note 69, at 139–40.

126 *See, e.g*, United States v. White, 401 U.S. 745, 752 (1971).

127 *See* Colb, *supra* note 69, at 141.

128 *See* Katz v. United States, 389 U.S. 347, 359 (1967); Colb, *supra* note 69, at 141.

129 *See* Colb, *supra* note 69, at 141.

130 *Id.* at 141–42.

people. Under the pretend friend line of cases, the user who becomes friends with an informant may have no Fourth Amendment protection because she had no reasonable expectation of privacy. On the other hand, even one's own real friend may give the police incriminating evidence. In the case of Facebook, users are in fact encouraged to report suspicious or illegal activity.[131] As noted above,[132] the Court has repeatedly ruled that there is no expectation of privacy in one's friends, so a social networking website user similarly does not have any Fourth Amendment protection against her friends' giving incriminating information to Government officials. Under *Katz* and the pretend friend cases, the social networking website user may receive little to no Fourth Amendment protection for information that she knowingly exposed to the public or information for which she has no reasonable expectation that the friend will relay to a third party.

Upon reviewing the pretend friend line of cases, one might ask whether *White* and *Katz* are inconsistent with each other.[133] The answer is both yes and no. *White* involves first party surveillance,[134] while *Katz* addresses third party surveillance.[135] The *White* Court believed that betrayal by one's friends is a reasonable expectation.[136] This notion is not without its criticism; according to Cornell Law School Professor Sherry F. Colb, a person's expectation of privacy should not be governed by her ability to detect pretend friends.[137] While an individual may assume a risk in confiding in a friend, there are limitations on that assumption of risk.[138] That is, the pretend friend may only do what one might assume a friend would do, and the confidence and expectation of privacy in one party is crucial to the inquiry.[139]

## VI. SOCIAL NETWORKING AND THE FOURTH AMENDMENT: ADDITIONAL CONSIDERATIONS

### A. *Youth and Social Networking*

While this Note attempts to highlight the various privacy concerns regarding social networking websites, research suggests that the social networking generation may not see a problem with a complete loss of privacy. For example, MTV and the Associated Press recently con-

131 *See How to Report Things*, FACEBOOK, http://www.facebook.com/report/ (last visited Oct. 19, 2012).

132 *See supra* note 122 and accompanying text.

133 *See* Colb, *supra* note 69, at 141.

134 *See* United States v. White, 401 U.S. 745, 746–47 (1971).

135 *See* Katz v. United States, 389 U.S. 347, 348 (1967).

136 *See White*, 401 U.S. at 746.

137 *See* Colb, *supra* note 69, at 141.

138 *See* Gouled v. United States, 255 U.S. 298, 305 (1921).

139 *See id.*

ducted a study regarding privacy issues relating to Facebook in which they surveyed users of the social networking website about the importance they placed on privacy.[140] In a poll of 1,355 people, fewer than half of those polled were "very upset" about the invasion of privacy on their social networking use.[141] This study suggests that many people may not have an expectation of privacy in the information they post online. If the youth of today have already relinquished the desire for a private life, it is difficult to expect a court to rule in favor of their privacy.

### *B. Obtaining a Warrant Against a Non-Suspect*

In *Zurcher v. Stanford Daily*,[142] the Supreme Court held that the Government may obtain a warrant to search for evidence even if the owner of the place to be searched is not suspected of being involved with the alleged criminal activity.[143] Under the *Zurcher* standard, the only concern is that the evidence will in fact be in the place to be searched.[144] However, *Zurcher* addressed the First Amendment concerns in searching a third party in a way that will compromise the First Amendment freedom of the press.[145] This standard could conceivably be applied to protect users' freedom of speech on social networking websites, from stating locations to discussing actions or posting pictures that could suggest that criminal activity is occurring or will occur.

### *C. The Seizure of Mere Evidence*

Even if the evidence on social networking websites is not the fruit of a crime, the photographs, location check-ins, tags, and status updates may be sufficient to justify further investigation, arrest, or eventually conviction. In *Warden v. Hayden*,[146] for example, the Supreme Court found that the right to seize evidence is not based on the Government's property interest, but rather on the Government and the public's interest in investigating and solving crime.[147] That interest allows for the seizure of "mere evidence," which is evidence that is not itself the fruit of a crime, but rather provides clues or direction in the commission of a

---

140 *See* Kashmir Hill, *Really? Half of Young People Not That Upset By Hacking of Their Facebook and E-mail Accounts*, FORBES (Oct. 12, 2011, 1:35 PM), http://www.forbes.com/sites/kashmirhill/2011/10/12/really-half-of-young-people-not-that-upset-by-hacking-of-their-facebook-and-e-mail-accounts/.

141 *Id.*

142 436 U.S. 547 (1978).

143 *Id.* at 567–68.

144 *See id.* at 554.

145 *See id.* at 563.

146 387 U.S. 294 (1967).

147 *See id.* at 304, 306.

crime.[148] Under the mere evidence standard, the Government is free to obtain all evidence of a crime.[149] In the context of social networking, the Government may search websites like Facebook, Twitter, and Foursquare in the hopes of learning more about the suspect's whereabouts or actions. However, this also means that the Internet user who may not be the primary suspect may also be subject to search. Government officials may thus seize this evidence under the *Zurcher* principle that one may be searched even if the officials have no reason to suspect the third party of committing the illegal act or assisting the suspect.

### *D. Standing and Fourth Amendment Suppression Claims*

In all Fourth Amendment cases, only the person with "standing," i.e., the person with the reasonable expectation of privacy, may argue for the suppression of illegally obtained evidence. In the social networking context, who has the expectation of privacy—the user or the social networking website? If the Government searched social networking websites for your information, could you even present a claim to suppress that evidence?

Under *Rakas v. Illinois*,[150] the Supreme Court's decision articulating Fourth Amendment standing, an individual has standing to argue for the suppression of unconstitutionally obtained evidence if she had a legitimate expectation of privacy in the place where the evidence was seized.[151] As in *Katz*, the person challenging the lawfulness of the search must have a subjective expectation of privacy in the place that the search occurred.[152] The person must also demonstrate that the expectation of privacy is one that society accepts as reasonable.[153]

Therefore, a social networking website user may argue that she has an expectation of privacy in the information shared online, but it is also arguable that the social networking website holds the privacy interest. This is because the terms of use of these websites give the websites the rights to information posted online, and the social networking websites control any information searched by the Government on those websites.[154] Thus, while social networking website users may want their information to remain private, they may not have the right to raise a claim if that information becomes publicly available or illegally searched by Government officials.

---

148 *See id.* at 300–01, 310.

149 *See id.*; *see also* FED. R. CRIM. P. 41(c) (stating that a warrant may be issued to search for and seize all evidence of a crime).

150 439 U.S. 128 (1978).

151 *Id.* at 135.

152 *See id.* at 149.

153 *See id.*

154 *See supra* Part III.B.

## CONCLUSION

As social networking websites become more popular, the legal implications concerning those websites increase. While the Fourth Amendment protects against unreasonable searches and seizures, the Supreme Court will not afford protection to anything it does not consider to be a search. Facebook, Twitter, and Foursquare all provide great opportunities to connect with friends and create new relationships,[155] but these opportunities may come at a price. The ordinary Internet user must consider the legal significance of posting private information to a public network. The 800 million Facebook users, 100 million Twitter users, and 10 million Foursquare users must stay constantly aware of the legality of their actions, especially if they write about those actions online or post photographs on public Internet websites. Additionally, while the Supreme Court may not endorse GPS-tracking,[156] Internet users may voluntarily opt-in to having their location tracked, whether that occurs through check-ins or the cookies placed on computers or smartphones.

Courts judge Fourth Amendment search claims by the *Katz* reasonable expectation of privacy standard, and this Note argues that social networking users cannot expect to maintain a reasonable expectation of privacy when they sign away their rights in privacy policies or post information for public consumption through their friends or any Internet viewers. The Fourth Amendment case law that has followed the *Katz* decision continues to use this framework, and many citizens have relinquished their privacy rights through public disclosure of information.

America may or may not be in the post-privacy era that Mark Zuckerberg describes.[157] It is true that youth do not value privacy as much as their elders, but their feelings may change when they realize that their entire lives can be traced on the Internet. Lawmakers are becoming more aware of the legal significance of social networking, and recent developments in Internet privacy laws are a step in the right direction. However, the only sure protection is awareness of the information one posts online and the image thus projected to Government officials. In the immortal words of Adele, they will "find someone like you."[158]

---

155 *See supra* notes 7–19 and accompanying text.

156 *See* United States v. Jones, 132 S. Ct. 945, 951–52 (2012).

157 *See* Popkin, *supra* note 87.

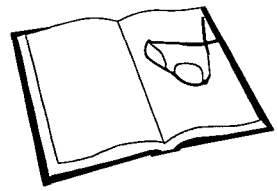
158 ADELE, SOMEONE LIKE YOU (Columbia 2011).

# ORDER THROUGH HEIN!

Get your missing back volumes and issues through Hein!

We have obtained the entire back stock, electronic, reprint and microform rights to . . .

## Cornell Journal of Law & Public Policy



Complete sets to date are available now!
We can also furnish single volumes and issues!

**BACK ISSUES ALSO AVAILABLE IN *HEIN-ON-LINE***
http://heinonline.org

HEIN
Fred B. Rothman & Co.
Acme-Nebrich Bookbindery
Fred O. Dennis & Co.
Metro Self-Storage
***Primus Inter Pares***

**WILLIAM S. HEIN & CO., INC.**
*Law Publisher / Serial & Subscription Agent / Micropublisher*
*New & Used Law Books / Preservation Printer / Bookbinder*
1285 Main Street, Buffalo, New York 14209
(716) 882-2600 • TOLL FREE (800) 828-7571 • Fax (716) 883-8100
E-Mail mail@wshein.com • Web Site www.wshein.com

# CORNELL LAW REVIEW

## FORTHCOMING ISSUE

**Volume 98** **March 2013** **Number 3**

ARTICLES



NOTES



Subscription & Order Requests:
*Cornell Law Review*
*Myron Taylor Hall*
*Ithaca, NY 14853-4901*

*Business Office (607) 255-3387*
*Fax (607) 255-7193*