DHS Investigations on Facebook and Other Online Social Networking Sites

BY RAJAT P. KUVER

Introduction

Internet privacy law in the context of social networking sites is an extremely complex area of law. At this moment, we simply do not know whether the government has the authority to conduct surveillance of Facebook, MySpace and other social networking sites. This article sets forth an argument that the government does not have that right and it will serve as an introduction to the Stored Communications Act (SCA) for immigration counsel.

Government surveillance of social networking sites is increasing. Therefore, it is important for immigration counsel to be aware that there are limits to government surveillance power. Counsel should point out those limits to officers who use information obtained from a client's social networking site. Counsel should also encourage clients to set high privacy settings on their social networking sites. Lastly, counsel should consider the possibility of federal litigation when a client's online information has been compromised.

In 2008, the U.S. Department of Homeland Security (DHS), U.S. Citizenship and Immigration Service (CIS), Office of Fraud Detection and National Security (FDNS), issued a memo indicating that it was using social networking sites to observe individuals suspected of fraudulent activities.[1] In 2011, DHS provided notice to the public that it proposes to establish a new security system based upon information received from social networking sites.[2]

In the future, we are likely to see immigration petition denials where there is some evidence obtained by the government from social networking sites. For example, an H-1B extension petition might be denied because an employee's Facebook page indicates that he is working at a different location than what is stated on the H-1B petition. A marriage-based immigrant visa petition might be denied because a client's Facebook page shows that he is not living with his wife.

Knowledge of the SCA is relevant to immigration counsel. For example, let us say you are litigating a denied immigrant or nonimmigrant visa petition in federal court, under the Administrative Procedures Act (APA).[3] If there is evidence that the government obtained information from your client's social networking site, you could also claim at least $10,000 plus litigation costs under the SCA. Section 2712 of the SCA gives a specific cause of action against the U.S. government and, therefore, issues of sovereign immunity would not apply. As a matter of strategy, adding a claim for damages and litigation costs under the SCA along with your APA claim might encourage the U.S. Attorney and/or DHS to settle your case out of court.

This article deals with three basic issues. What steps is the government taking to investigate social networking sites? Do such investigations of social networking sites violate the SCA? If they do, then what are the remedies?

DHS Surveillance

The 2008 CIS memo entitled, "Social Networking Sites and Their Importance to FDNS,"[4] states that:

> Social networking sites such as MySpace, Facebook, Classmates, Hi-5, and other similar sites are designed to allow people to share

---

[1] The FDNS memo was issued in response to a Freedom of Information Act request filed by the Electronic Frontier Foundation. "Applying for Citizenship? U.S. Citizenship and Immigration Wants to Be Your 'Friend'," Jennifer Lynch, Electronic Frontier Foundation, October 12, 2010, https://www.eff.org/deeplinks2010/10/applying-citizenship-u-s-citizenship-and.

[2] 76 Fed. Reg. 5603 (Feb. 1, 2011).

[3] The Administrative Procedures Act (APA) provides for judicial review of final agency decisions. 5 U.S.C. 702, 706. The APA "commands reviewing courts to 'hold unlawful and set aside' agency action that is 'artibrary, capricious, an abuse of discretion, or otherwise not in accordance with law.' " Thomas Jefferson Univ. v. Shalala, 512 U.S. 504, 512 (1994) (quoting 5 U.S.C. 706(2)(A)).

[4] "FDNS" refers to the Office of Fraud Detection and National Security of the United States Citizenship and Immigration Services. "Social Networking Sites and Their Importance to FDNS," U.S. Department of Homeland Security, U.S. Citizenship and Immigration Services, p. 1 (undated).

> their creativity, pictures, and information with others. ... Narcissistic tendencies in many people fuels a need to have a large group of "friends" link to their pages and many of these people accept cyber-friends that they don't even know. This provides an excellent vantage point for FDNS to observe the daily life of beneficiaries and petitioners who are suspected of fraudulent activities. ...[5]

The memo also says, "This social networking gives FDNS an opportunity to reveal fraud by browsing these sites to see if petitioners and beneficiaries are in a valid relationship or are attempting to deceive CIS about their relationship."[6] The FDNS memo provides no guidelines to officers on how or when to proceed with such online investigations.

On February 1, 2011, DHS provided notice to the public that it proposes to establish a new security system called the "Department of Homeland Security Office of Operations Coordination and Planning—004 Publicly Available Social Media Monitoring and Situational Awareness Initiative System of Records."[7] The Office of Operations Coordination and Planning (OPS) National Operations Center (NOC) leads that initiative.[8]

The purpose of the system of records is to allow DHS to provide "situational awareness."[9] The law defines "situational awareness" as "information gathered from a variety of sources that, when communicated to emergency managers and decision makers, can form the basis for incident management decision-making."[10]

[5] "Social Networking Sites and Their Importance to FDNS," U.S. Department of Homeland Security, U.S. Citizenship and Immigration Services, p. 1 (undated).

[6] "Social Networking Sites and Their Importance to FDNS," U.S. Department of Homeland Security, U.S. Citizenship and Immigration Services, p. 1 (undated).

[7] 76 Fed. Reg. 5603 (Feb. 1, 2011).

[8] This Federal Register notice was provided by DHS to the public pursuant to the Privacy Act of 1974 (5 U.S.C. 552a, Pub. L. 93-579, Sec. 3, Dec. 31, 1974, 88 Stat. 1897). This article will not cover the Privacy Act because that Act applies to information that is maintained in a government "system of records". By contrast, this article focuses on whether the government has the power to "access" information rather than whether the government has the authority to create a system of records to "store" that information.

[9] 76 Fed. Reg. 5603 (Feb. 1, 2011).

[10] Section 515 of the Homeland Security Act (6 U.S.C. 321d(b)(1), Pub. L. 107-296, title V, Sec. 515, as added Pub. L. 109-295, title VI, Sec. 611(13), Oct. 4, 2006, 120 Stat. 1409); Federal Register, Vol. 76, No. 21, February 1, 2011, p. 5603.

The CIS memo and the DHS Initiative indicate that the government is taking steps to access and store information from social networking sites.

Social Networking Sites and Facebook

Social networking sites are Internet-based services where individuals communicate with each other about shared interests. Facebook is the most popular social networking site on the Internet.[11] A Facebook user who does not set his or her privacy settings, will have the following information available on his or her Facebook page:

1. The Facebook "Wall" — contains messages to and from the user to other Facebook users;
2. Biographical information such as place of employment, educational background, residence (city and state), birthplace (city and country), and marital/relationship status;
3. Photos uploaded by the user onto his or her Facebook page;
4. A list of the user's Facebook "friends."

Many Facebook users have all of this information available on their Facebook page. However, some users set their privacy settings at a higher level and they can make all or some of the information listed above private. In order to see private information, a "friend request" would have to be sent to the Facebook user. If the user accepts the "friend request," then the information would be available to that specific "friend."

The Stored Communications Act

The means by which government agents can obtain information contained in "electronic storage" is found in the Stored Communications Act (SCA). The SCA is part of the Electronic Communications Privacy Act (ECPA) and is codified at 18 U.S.C. 2701 to 2712.[12]

The SCA provides a cause of action against anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided...and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage."[13] "Electronic storage" means either "temporary, intermediate

[11] There were over 845 million monthly active users on Facebook at the end of December 2011. http://newsroom.fb.com/content/default.aspx?NewsAreaId=22.

[12] Pub. L. 99-508, title II, Sec. 201[(a)], Oct. 21, 1986, 100 Stat. 1860.

[13] 18 U.S.C. 2701(a)(1), 2707(a).

storage ... incidental to ... electronic transmission," or "storage ... for purposes of backup protection.[14]

In *Crispin v. Audigier, Inc.*,[15] it was held that the SCA applies to social networking sites, such as Facebook and MySpace. Facebook and MySpace private messages which have not been opened by their recipients fall within the definition of "temporary, intermediate storage" under Section 2510(17)(A). Facebook and MySpace messages that have been opened and retained by their recipients are stored "for purposes of backup protection" under Section 2510(17)(B). Facebook wall postings and MySpace comments are also stored "for purposes of backup protection" under Section 2510(17)(B).

A. Standing

Standing requires a plaintiff to prove (1) that it has actual injury or will suffer actual injury as a result of defendant's actions; (2) that the injury can be traced to the challenged actions; and (3) that the injury is likely to be redressed by a favorable decision.[16] Furthermore, the interest sought to be protected must be arguably within the zone of interests protected or regulated by the statute in question.[17]

In response to an SCA action, the government may argue that the SCA sets limits on the government's power to obtain stored information from "providers" of communication services.[18] Arguably, a social network site user is not a "provider" and, therefore, would have no standing under the SCA.

However, 18 U.S.C. 2712(a) states that, "Any person who is aggrieved by any willful violation of this chapter ... may commence an action...against the United States ...." The case of *Jewel v. National Security Agency*[19] involved a class action lawsuit brought by Carolyn Jewel against the federal government and government officers, in their official and personal capacities, for violating the SCA and other statutes. Jewell alleged that AT&T in collaboration with the National Security Agency (NSA) diverted her Internet traffic to the NSA. The Ninth Circuit held that Jewell had standing under the SCA which creates a private right of action for claims of illegal surveillance.

Furthermore, the district court in *Crispin* discussed SCA standing and held that, "...an individual has a personal right in information in his or her profile and inbox on a social networking site and his or her webmail inbox in the same way that an individual has a personal right in employment and bank records." Therefore, both the statute and case law indicate that a user of a social networking site would have standing under the SCA.

B. User Consent and Authorized Conduct

Under 18 U.S.C. 2701(c)(2), there is no SCA violation if there is "... conduct authorized ... by a user of that service with respect to a communication of or intended for that user ..." Therefore, in response to an SCA lawsuit, the government could argue that a Facebook user who has accepted a "friend" request from an undercover officer falls within the exception provided by 18 U.S.C. 2701(c)(2) as "conduct authorized by a user."

However, in Theofel v. Farey-Jones,[20] the Ninth Circuit held that, Section 2701(c) "provides no refuge for a defendant who procures consent by exploiting a known mistake that relates to the essential nature of his access."[21] The court applied trespass law to Section 2701(c) and stated:

> Like the tort of trespass, the Stored Communications Act protects individual's privacy and proprietary interests...Just as trespass protects those who rent space from a commercial storage facility to hold sensitive documents, cf. Prosser and Keeton on the Law of Torts, Section 13, at 78 (W. Page Keeton ed., 5th ed 1984), the Act protects users whose electronic communications are in electronic storage with an ISP or other electronic communications facility.
>
> A defendant is not liable for trespass if the plaintiff authorized his entry. *See* Prosser & Keeton Section 13, at 70. But "an overt manifestation of assent or willingness would not be effective...if the defendant knew, or probably if he ought to have known in the exercise of reasonable care, that the plaintiff was mistaken as to the nature and quality of the invasion intended." Id. Section 18, at 119; cf. Restatement (Second) of Torts Sections 173, 892B(2). Thus, the busybody who gets permission to come inside by

---

[14] 18 U.S.C. 2510(17).

[15] 717 F. Supp. 2d 965 (C.D. Cal. 2010).

[16] Massachusetts v. EPA, 127 S.Ct. 1438 (2007).

[17] National Credit Union Administration v. First National Bank and Trust Co., 118 S.Ct. 927, 933 (1998).

[18] 18 U.S.C. 2307(a) and (b).

[19] 673 F.3d 902 (9th Cir. 2011).

[20] 359 F.3d 1066 (9th Cir. 2004).

[21] Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004).

posing as a meter reader is a trespasser. J.H. Desnick, M.D., Eye Servs., Ltd. v. ABC, 44 F.3d 1345, 1352 (7th Cir. 1995). So too is the police officer who, invited into a home, conceals a recording device for the media. *Cf* Berger v. Hanlon, 129 F.3d 505, 516-17 (9th Cir. 1997), *vacated* 526 U.S. 808 (1999), *reinstated in relevant part*, 188 F.3d 1155, 1157 (9th Cir. 1999).[22]

Whether or not there has been a trespass should be examined in the light of the privacy settings of a particular social networking site. For example, a Facebook user's page is not available to simply any member of the public using the Internet. In order to see a Facebook page, an individual must be a member of Facebook. Only by registering with Facebook can one have access to a Facebook user's information. Furthermore, if the Facebook user has made his or her information private, then one must be accepted as a user's "friend" before the user's information is accessible.

Individuals need to register to use Facebook. In order to register, Facebook requires a user to agree to the terms of its "Statement of Rights and Responsibilities (SRR)".[23] The SRR states, in part, that by using or accessing Facebook, a user agrees to these statements:

1. You will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission.
2. If you collect information from users, you will obtain their consent, make it clear you (and not Facebook) are the one collecting their information, and post a privacy policy explaining what information you collect and how you will use it.[24]

The first requirement means that law enforcement cannot use a false name to communicate with a Facebook user. The second requirement means that law enforcement cannot collect information about a user without that user's informed consent. Doing so would violate the SRR (also referred to as the "Terms of Service").

If an undercover officer violates the SRR, would that constitute an "intentional access without authorization" in violation of Section 2701(a)(1) of the SCA? The district court *United States v. Drew*[25] stated that, "Within the breach of contract approach, most courts that have considered the issue have held that a conscious violation of a website's terms of service/use will render the access unauthorized and/or cause it to exceed authorization.[26] However, the *Drew* case dealt with the Computer Fraud and Abuse Act (CFAA)[27] rather than the SCA. Nevertheless, Section 1030(a) of the CFAA and Section 2701(a) of the SCA both make it an offense for anyone to "intentionally access without authorization" and, therefore, the findings in *Drew* might also be useful in the SCA context.[28]

That a Facebook user accepts a "friend" request from law enforcement should not constitute "conduct authorized by a user" under 18 U.S.C. 2701(c) because (a) the government would be procuring the user's consent by exploiting a known mistake that relates to the essential nature of his access in violation of *Theofel* and (b) the government would be violating the terms of service agreement of the social networking site provider in violation of *Drew*. To date, however, many of these issues remain unresolved by the courts.

C. Communication Readily Accessible to the General Public

18 U.S.C. 2511(2)(g)(i) says that, "It shall not be unlawful under this chapter or chapter 121 of this title for any person to intercept or access an electronic communication that is readily accessible to the general public."[29] Chapter 121 refers to the SCA. Therefore, under Section 2511(2)(g)(i), it would be lawful to access an electronic communication under the SCA if that communication was readily accessible to the general public.

The remaining question is whether electronic communication contained in social networking sites is "readily accessible to the general public." The district

---

[22] Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004).

[23] http://www.facebook.com/legal/terms.

[24] http://www.facebook.com/legal/terms.

[25] 249 F.R.D. 449 (C.D. Cal. 2009).

[26] United States v. Drew, 249 F.R.D. 449 (C.D. Cal. 2009), *citing* Southwest Airlines Co. v. Farechase, Inc., 318 F. Supp. 2d 435, 439-40 (N.D. Tex 2004); Nat'l Health Care Disc., Inc., 174 F. Supp. 2d at 899; Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 247-51 (S.D.N.Y. 2000), *aff'd*, 356 F.3d 393 (2d Cir. 2004); Am.Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 450 (E.D. Va. 1998); EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 62-63 (1st Cir. 2003).

[27] 18 U.S.C. 1030, Pub. L. 98-473, title II, Sec. 2102(a), Oct. 12, 1984, 98 Stat. 2190.

[28] This article deals with the SCA rather than the CFAA because the SCA provides a private cause of action against the government and also an CFAA claim against the government could face sovereign immunity hurdles.

[29] 18 U.S.C. 2511(2)(g).

court in *Crispin v. Audigier, Inc.*,[30] answered that question. The court held that Facebook "wall postings" and MySpace "comments" were not strictly "public" because they are accessible only to those individuals which a user selects.[31]

In *Crispin*, the court noted that judicial precedent and legislative history establish that the SCA was intended to reach a "private" BBS (bulletin board service)..[32] The court stated,

> ... a completely public BBS does not merit protection under the SCA. Kaufman at 5...S. Rep. No. 99-541, at 36 ("The bill does not for example hinder the development or use of 'electronic bulletin boards' or other similar services where the availability of information about the service, and the readily accessible nature of the service are widely known and the service does not require any special access code or warning to indicate that the information is private. To access a communication in such a public system is not a violation of the Act, since the general public has been "authorized" to do so by the facility provider.[33]

However, the court found that Facebook and MySpace permit wall messages and comments to be viewed by only those with access to the user's profile page. Therefore, there was no basis for distinguishing between a restricted-access BBS and a user's Facebook wall or MySpace comments. There similarly was no basis for distinguishing between Facebook's and MySpace's private messaging, on the one hand, and traditional web-based email on the other.[34]

With respect to private messaging, the court held that such communications are inherently private and such stored messages are not accessible to the public. As to wall postings, the court held that it will depend on the user's privacy settings. If the user has made them private, then they are not accessible to the public.[35] If the user has not made his wall postings private, then an SCA claim against the government might be futile.

The SCA Remedy

18 U.S.C. 2712 states that, "Any person who is aggrieved by any willful violation of this chapter ... may commence an action in United States District Court against the United States to recover money damages ... the Court may assess as damages—(1) actual damages, but not less than $10,000, whichever amount is greater; and (2) litigation costs, reasonably incurred."

Actual damage is a prerequisite to recover.[36] In the employment-based petition context, actual damages could be petitioner's lost business income resulting from the employee's inability to work. For the family-based petition, actual damages may be difficult to prove. However, if there is some actual damage, then at least the statutory $10,000 amount could be claimed.

18 U.S.C. 2712(b) sets for the procedure for a civil action against the U.S. Section 2712(b)(1) requires that "Any action against the United States under this section may be commenced only after a claim is presented to the appropriate department or agency under the procedures of the Federal Tort Claims Act." Tort Claims Procedure is set forth in 28 U.S.C. 2671 to 2680. Section 2675(a) states that, "An action shall not be instituted upon a claim against the United States for money damages...unless the claimant has first presented the claim to the appropriate Federal agency and his claim shall have been finally denied by the agency in writing...The failure of an agency to make a final disposition of a claim within six months after it is filed shall...be deemed a final denial of the claim..." Furthermore, 28 U.S.C. 2672 states that, "The head of each Federal agency or his designee ... may ... compromise, and settle any claim for money damages against the United States ... caused by the negligent or wrongful act or omission of any employee of the agency while acting within the scope of his office or employment ..."

Therefore, in order to bring a SCA claim, a Federal Torts Claim filing must be first made to DHS. The DHS might settle or they might deny the claim or they might

---

[30] 717 F. Supp. 2d 965 (C.D. Cal. 2010).

[31] Crispin v. Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010).

[32] Crispin v. Audigier, Inc., 717 F. Supp. 2d 965, 981 (C.D. Cal. 2010), *citing* United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003). *See also* Konop, 302 F.3d at 875; Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457, 462 (5th Cir. 1994).

[33] Crispin v. Audigier, Inc., 717 F. Supp. 2d 965, 981 (C.D. Cal. 2010).

[34] Crispin v. Audigier, Inc., 717 F. Supp. 2d 965, 981-982 (C.D. Cal. 2010).

[35] Crispin v. Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010).

[36] Van Alstyne v. Electronic Scriptorium, Ltd., 560 F.3d 199, 205 (4th Cir. 2009); Cornerstone Consultants, Inc., v. Production Input Solutions, LLC, 789 F. Supp. 2d 1029, 1043 (N.D. Iowa 2011).

not make any decision. If no decision is made within six months, then the claim is deemed denied and an SCA claim can be filed.

Under 18 U.S.C. 2712, an SCA claim must be brought within two years of the date upon which the claimant first had a reasonable opportunity to discover the violation. An SCA claim can also be brought within six months after the mailing of a final denial of the claim by the agency to which it was presented.

Conclusion

What was once considered private information is now readily available on popular social networking sites on the Internet. DHS is taking steps to access information from social networking sites as well as store information gathered from those sites into databases. However, the government's power to conduct undercover investigations and/or collect information from social networking sites is restricted by the Stored Communications Act (SCA). Furthermore, an SCA claim can be bolstered with a claim under the Fourth Amendment to the U.S. Constitution.[37] However, whether there is a "reasonable expectation of privacy"[38] in social networking site communications under the Fourth Amendment to the U.S. Constitution remains an unresolved question and deserves an entirely separate article.[39] Immigration counsel should, nevertheless, be aware that there are "statutory" limits to government investigatory power on social networking sites. Counsel should consider pointing out these limits to DHS officers during immigration interviews. Counsel should also consider being proactive by informing clients to be aware of their privacy settings on social networking sites. Lastly, counsel should consider adding an SCA claim for damages in any future federal litigation where government surveillance of a social networking site is involved.

*****

Rajat P. Kuver has been practicing immigration law for over seventeen years. He received his J.D. degree from Wayne State University in Detroit, Michigan, and his L.L.M. in international business law from Central European University in Budapest, Hungary. He was an adjunct professor of business law at Golden Gate University in San Francisco, California, from 2003 to 2011. His previous publication and lectures involve security and technology issues such as export licensing. His private practice is located in Cupertino and Palo Alto, California.

---

[37] The Fourth Amendment states, "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 probably cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

[38] The Fourth Amendment "reasonable expectation of privacy" test was set forth in Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan J., concurring).

[39] "Balancing the Scales of Justice: Undercover Investigations on Social Networking Sites," Chahal, Shirin, J. On Telecomm. & High Tech. L., Vol. 9, 285, University of Colorado Law School (2011).