The Ascendance of Social Media as Evidence

BY ADRIAN FONTECILLA

Social media has become a pillar of communication in today's society and, consequently, it factors into the majority of government investigations or criminal litigation in some respect. Social media evidence can include countless types of content, and the amount of social media evidence available is growing exponentially as law enforcement, lawyers, and the law itself struggle to keep up with its evolution.

The Importance of Social Media
The use of social media is widespread. Ninety-one percent of today's online adults use social media regularly, and “social media has overtaken porn as the #1 activity on the Web.” (Eric Qualman, Social Media Video 2013, Socialnomics (2012), available at http://www.socialnomics.net/2013/01/01/social-media-video-2013/) In fact, people spend more time on social networks than any other category of websites, accounting for 20 percent of their time spent on PCs and 30 percent of their mobile use time. (Nielsen, State of the Media: Social Media Report 2012 (2012), available at http://tinyurl.com/d3s4z6l; Brian Honigman, 100 Fascinating Social Media Statistics and Figures from 2012, Huffington Post (Nov. 29, 2012).)

There are hundreds of social networking websites, and their users are constantly creating massive amounts of data. This has resulted in a digital gold mine of potential evidence: profiles, lists of friends, group memberships, messages, chat logs, tweets, photos, videos, tags, GPS locations, “likes,” check-ins, login timetables, and more. Not surprisingly, government agencies regularly seek social media evidence because—whether obtained through public sources, a subpoena, or a warrant—the effort can yield large volumes of damaging statements or incriminating photos, among other evidence.

Accessing Social Media Evidence
Given the amount of information publicly available, and the avenues that the government has to seek out such information, the government often does not even need a search warrant, subpoena, or court order to obtain social media evidence. For example, a defendant in Kentucky was jailed after he posted to Facebook a photo of himself siphoning gas from a police car. Another defendant burgled a Washington, D.C., home and then used the victim’s laptop to post to the victim’s Facebook page a picture of himself wearing the victim’s coat and holding up the victim’s cash. The photo was later used to secure a guilty plea from the defendant. (See Eric Larson, 8 Dumb Criminals Caught through Facebook, Mashable (Dec. 12, 2012), http://tinyurl.com/cg9w897.)

In addition to searching for publicly available evidence, government agents pierce the privacy settings of a person’s social media account by creating fake online identities or by securing cooperating witnesses to grant them access to information. Recently, federal authorities relied heavily on social media to build their case against four defendants who were allegedly involved in an al-Qaeda-inspired terrorist cell based in California. The criminal complaint, which included a section titled “Defendants’ Social Media,” described how the investigators used an “online covert employee” who posed as a terrorism sympathizer to elicit damaging statements from the defendants and relied on the social media content that each defendant “liked,” “shared,” or commented on. (Criminal Complaint, United States v. Kabir, No. ED12-0431M (C.D. Cal. Nov. 16, 2012).)

Social media evidence is a new frontier of criminal proceedings, raising unique legal challenges, including a defendant’s constitutional rights in material maintained by social media companies.

SCA and Defendants’ Rights
The Stored Communications Act (SCA) governs the ability of governmental entities to compel service providers, such as Twitter and Facebook, to produce social media evidence. (Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 977 (C.D. Cal. 2010) (aplying SCA to subpoenas issued to Facebook and MySpace while recognizing that no courts “have addressed whether social networking sites fall within the ambit of the statute”).)

But, in United States v. Warshak, 631 F.3d 266 (6th Cir. 2010), the Sixth Circuit challenged the SCAs constitutionality, holding that “government agents violated the Fourth Amendment when they obtained the contents of [the defendant’s] emails” without a warrant, and added that “to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional.” (Id. at 288.) The court reasoned that “[o]ver the last decade, email has become ‘so pervasive that some persons may consider [it] to be an essential means or necessary instrument[] for self-expression, even self-identification’” and that therefore “email requires strong protection under the
Fourth Amendment.” (Id. at 286 (alterations in original)). Noting that e-mail was analogous to a phone call or letter and that the Internet service provider was the intermediary that made e-mail communication possible—the functional equivalent of a post office or telephone company—the court concluded that given “the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection.” (Id. at 285–86).

The SCA, which was passed in 1986, has not been amended to reflect society’s newer technologies. And Congress made clear that changing the law will require extended consideration when, on December 24, 2012, the Senate removed from proposed legislation an amendment to the SCA that would have prevented authorities from viewing a person’s e-mail messages without obtaining a warrant. (Netflix Social Sharing Bill Passes without Email Privacy Protection, HUFFINGTON POST (Dec. 26, 2012)). Consequently, courts will play a key role in clarifying how the SCA applies to e-mails as well as the social media that has rapidly become as pervasive as e-mail.

For example, a New York appellate court will soon rule regarding Twitter’s appeal of two court orders in the prosecution of an Occupy Wall Street protestor. The trial court held that the defendant lacked standing to move to quash the government’s third-party subpoenas to Twitter for his account records and that his tweets were not protected by the Fourth Amendment; the court also denied Twitter’s motion to quash the government’s subpoenas. (People v. Harris, 949 N.Y.S.2d 590, 597 (Crim. Ct. 2012)).

Twitter appealed, arguing that the defendant has standing because he has a proprietary interest in his tweets, pointing to the express language of Twitter’s Terms of Service. (Brief for Non-Party Movant-Appellant, People v. Harris, No. 2011-80152 (N.Y. App. Div. Aug. 27, 2012), 2012 WL 3867233, at *12–13.) Moreover, Twitter claimed that the defendant’s tweets are protected by the Fourth Amendment, primarily because the government conceded that the tweets it sought were not made public by the defendant. (Id.) And, if a defendant has a reasonable expectation of privacy under the Fourth Amendment in his or her nonpublic e-mails, not affording that same protection to users’ nonpublic tweets would create “arbitrary line drawing.” (Id. at *18, *21.)

Twitter’s appeal is pending, but Twitter turned over the data pursuant to a subsequent court order and the defendant pleaded guilty in December 2012. (Russ Buettner, A Brooklyn Protester Pleads Guilty after His Twitter Posts Sink His Case, N.Y. TIMES (Dec. 12, 2012)).

The line-drawing concerns expressed by Twitter in its Harris brief were implicated in United States v. Meregildo, 2012 WL 3264501, at *2 (S.D.N.Y. Aug. 10, 2012), where the defendant set the privacy settings on his Facebook account so that only his Facebook “friends” could view his postings. The government obtained incriminating evidence through a cooperating witness who was Facebook “friends” with the defendant. The defendant moved to suppress the evidence, arguing that the government had violated his Fourth Amendment rights. The court found:

Where Facebook privacy settings allow viewership of postings by “friends,” the Government may access them through a cooperating witness who is a “friend” without violating the Fourth Amendment. While [the defendant] undoubtedly believed that his Facebook profile would not be shared with law enforcement, he had no justifiable expectation that his “friends” would keep his profile private. And the wider his circle of “friends,” the more likely [the defendant’s] posts would be viewed by someone he never expected to see them. [The defendant’s] legitimate expectation of privacy ended when he disseminated posts to his “friends” because those “friends” were free to use the information however they wanted—including sharing it with the Government. (Id.)

Other courts have similarly concluded that individuals have “a reasonable expectation of privacy to [their] private Facebook information and messages.” (R.S. ex rel. S.S. v. Minnewaska Area Sch. Dist. No. 2149, 2012 WL 3870868, at *12 (D. Minn. Sept. 6, 2012)).

But using privacy setting distinctions to determine social media users’ constitutional rights may result in arbitrary line drawing that may become outdated as social media evolves. Indeed, with Facebook’s customizable and post-specific privacy settings, a person sharing a message by posting it on another user’s wall can actually make it as private as information shared via a Facebook message. Ultimately, because an expectation of privacy under the Fourth Amendment is partly a function of whether “society [is] willing to recognize that expectation as reasonable,” social media’s rapid proliferation may influence the privacy protections afforded to social media evidence in the future. (See United States v. Warshak, 631 F.3d 266, 284–85 (6th Cir. 2010) (“[T]he Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish.”).) In the meantime, social media users create warehouses of potential evidence while courts struggle to define how this information fits into existing legal paradigms of constitutional protections and the SCA.