Bloomberg Law Reports® Privacy & Information

Information Gathering and Social Networks: Minimizing Exposure in the Digital Age

Erin Reid and Connie Pendleton, Davis Wright Tremaine

Social networking websites can serve as first impressions for employers, investors, friends, and potential romantic partners. From Twitter to Facebook to YouTube, use of social networking sites has become ubiquitous. Yet, for all the talk of social networking and social media, many users lack a clear understanding of the ramifications of using such websites. So, what is online social networking and how does it work? As use of social networking sites grows, what kind of legal exposure could sites face for programs and policies that disclose user information? Will online social networking change how courts, lawyers and juries conduct discovery, prepare for trial, and deliberate? This article examines these questions in turn.

Social Networking 101

Online social networking sites allow users – through personal computers or mobile phones – to share ideas, activities, events, and interests within their individual social networks – and all typically for free. Social networking sites run the gamut: there are sites devoted to dating and meeting new people (*e.g.*, Nerve, Match, eHarmony), sites that offer users the opportunity to connect with friends and family members (*e.g.*, Facebook, MySpace, Ping), sites for professional networking (*e.g.*, LinkedIn, Sermo, INmobile), and sites devoted to information sharing (*e.g.*, Twitter, Redditt, Digg). Online social media usage has risen dramatically over the last three years – 230 percent since 2007, according to a recent Simmons New Media Study.[1] Nearly 66 percent of Americans online report using a social networking site, with nearly half of that group accessing sites multiple times a day.[2] Use of social networks is not just for the young. Forty-one percent of online adults over the age of 50 report making monthly visits to social networking sites.[3] As of April 26, 2010, 46 percent of online adults in the U.S. reported visiting Facebook within the last 30 days, according to the Simmons Study.[4]

Facebook is by far the most popular social networking site worldwide, with over 500 million users spending an estimated 700 billion minutes a month sharing personal updates and photos at the site.[5] But online social networking is exploding in other areas as well. Twitter, a popular instant messaging website that allows users to send short messages to online "followers," reported in February 2010 that its users were sending over 50 million "tweets" a day.[6] YouTube users upload 24 hours of video footage each minute and watch over two billion videos a day on the video-sharing site.[7]

Social networks gather a range of information from users – from information users provide directly to the site, to information revealed when users interact with the site, to information gleaned from users' interaction with third parties.

User-provided information: Facebook's privacy policy, like that of its competitors, discloses the types of information it collects from users.[8] This information includes personal data users provide on the website (such as name, e-mail address, gender, and birth date), content users share (such as when a user updates their status, shares a link, makes a comment, sends a message, or uploads or records video), transactional information regarding payments or purchases made on the site, the e-mail addresses of individuals in a user's social network, and information provided by other users (such as when a friend "tags" a user in a picture, provides friend details, or indicates a relationship with the user).

Information generated through site interaction: Social networking sites also collect information generated by user interaction with the site, including cookie information (text stored on a user's computer, mobile phone or other device containing information about the user's Internet usage), the type of device and web browser used to access the site, and the user's location. Social networking sites also keep track of use of their the sites – logging when users post content, indicate they like a post, or connect with an application.

Information from third parties: Finally, social networks collect information from third parties about user interaction with third-party applications and websites. Third-party applications – such as FarmVille, a real-time farm simulation game available as a Facebook application in which users manage a virtual farm by planting, growing, and harvesting virtual crops and trees, and raising livestock – provide information to social networking sites about users' usage history. Advertisers also share conversion tracking data detailing users' response rates to advertising posted on the website.

Technological advances have made use of social networks and social media ubiquitous. As consumers engage in increasing amounts of social networking, the amount of personal, private data they disclose will continue to grow.

Risky Behavior

Technological advances have often been perceived to threaten privacy. In their seminal article on privacy in 1890, Samuel Warren and Louis Brandeis wrote of the dangers that instant photography and the tabloid press posed to society, warning "numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[9] Flash forward a hundred years and the public and lawmakers are expressing many of the same privacy concerns. At its core, the debate surrounding privacy and networking sites concerns who controls the disclosure of personal, private information. Following a string of high profile data breaches and unpopular programs launched by Twitter, Google and Facebook, public pressure is mounting for regulators to take action.

Twitter: In a recent ruling by the Federal Trade Commission, *In Re Matter of Twitter*, the FTC and Twitter entered into a consent order that requires Twitter to implement a variety of security measures with respect to its users' "nonpublic consumer information."[10] The FTC probe stemmed from two highly publicized security breaches in January and April of 2009 where hackers gained unauthorized administrative control of Twitter. In the first breach, a hacker was able to use an automated password guessing tool to gain access. Using that password, the hacker reset several passwords and posted them on a website accessible to the general public. Other intruders used the fraudulently reset passwords to send phony tweets from nine user accounts, including the account of then President-elect Barack Obama.[11] In a second breach, a hacker gained access to Twitter's administrative password, reset a user's password and accessed other Twitter users' nonpublic information and tweets. Once the consent order takes effect, Twitter will be barred for 20 years from misleading consumers about the extent to which it protects the security, privacy, and

confidentiality of nonpublic consumer information.[12] Twitter also will be required to establish and maintain a comprehensive information security program.[13]

Google: In February 2010, Google, owner of popular web-based e-mail program, Gmail, announced that it would be rolling out "Google Buzz," a social networking and messaging tool integrated into Gmail. Buzz, designed to function like Facebook and Twitter, allows users to leverage their Google contacts through a system of social updates. After a user publishes an update to Buzz, the information would not only be available to the user's contact list, it would also be searchable on Google. In addition, when accessed through a mobile device with GPS technology, Buzz uses the location-aware capabilities built into sites such as Google Maps to determine a user's location, map those coordinates to an intersection or restaurant, and then publish that information to all the contacts in the user's address book.

When Google launched Buzz, the company automatically signed up all Gmail users.[14] Within a week, Gmail users filed a class action lawsuit against Google in federal district court in California.[15] In addition, the Electronic Privacy Information Center (EPIC) filed a complaint with the FTC alleging that the social networking application caused "clear harms to service subscribers" because the application "violated user expectations, diminished user privacy, contradicted Google's own privacy policy, and may have also violated federal wiretap laws."[16] Gmail users criticized Google for automatically drawing their e-mail contacts into a social network and enrolling users in the program with no chance to opt-out before their private data was shared with their e-mail contacts.[17] Google apologized to users and is defending the class action.[18] To date, the FTC has not responded to EPIC's complaint.

Facebook: In 2007, Facebook launched Beacon, an online advertising system that sent data from external websites to Facebook for targeted advertising so users could share details about their activities with friends. Facebook cookies and a web bug on third-party websites tracked Facebook users' purchases and other activities on more than 40 participating websites, including Blockbuster, Fandango, Overstock and eBay. If the Beacon function was engaged, a message would appear about a purchase on the users' friends' newsfeeds, sometimes with unfortunate consequences. Sean Lane's wife inadvertently found out about a jewelry purchase her husband was to surprise her with when she read on her Facebook newsfeed that "Sean Lane bought 14k White Gold 1/5 ct Diamond Eternity Flower Ring from overstock.com."[19] Sean Lane and other Facebook users and privacy advocates protested the program, filing a class action suit against the website for allegedly disclosing members' personal information without consent.[20] In 2009, Facebook denied any wrongdoing but settled the lawsuit and announced it would shut down the program.[21] In June of 2010, the company was hit with three separate lawsuits alleging that it improperly shared users' information with advertisers.[22] Facebook has denied all allegations.

Social Networking Goes to Washington

Few, if any, of the federal and state laws that govern privacy apply to the types of personal data disclosed on social networking sites. Existing laws prohibit companies from disclosing Social Security numbers and other confidential financial account information or from using personal information obtained from children. But social networking sites often contain sensitive, private, non-financial information about users, such as gender, race, age, number of children, education level, geographic location, internet viewing habits, household information, and other non-financial personal information.

Regulators and legislators in Washington are increasingly scrutinizing the data collection and use policies of social networking sites. The FTC and members of Congress have signaled their intentions

to examine the issue. In March 2010, the FTC announced plans to seek public comment on whether the Children's Online Privacy Protection Act (COPPA) should be changed to reflect technological changes to the online environment, such as mobile communications, interactive television, interactive gaming, and other interactive media.[23]

During the last two weeks of the 2009-2010 legislative session, House and Senate committees held hearings to discuss new baseline standards for online privacy protection. On July 22, 2010, the House Energy and Commerce Subcommittee on Commerce, Trade and Consumer Protection held a hearing to discuss privacy legislation proposed by Rep. Bobby Rush (D-IL) and Rep. Rick Boucher (D-VA). Representative Rush's bill, H.R. 5777, titled "the Best Practices Act," and Representative Boucher's untitled, draft legislation would create a new series of regulatory requirements for social networking sites that collect user information. Under both bills, social networking sites would be required to get users' permission before collecting "sensitive information." In the Rush bill, sensitive information covers not just medical, sexual, religious and financial information, but race and ethnicity, precise geolocation, and biometrics. Under the Rush bill, social networking sites that share other "covered information" with third parties – including personal information, IP addresses, and unique persistent identifiers associated with an individual's computer or other device – would be required to obtain user consent prior to disclosure to third parties. The bill is designed to induce companies to join an FTC-approved safe harbor, under which they could use opt-out models and receive some relief from proposed uncapped private causes of action. Businesses or individuals who fail to abide by the FTC's regulatory requirements would face fines of up to $5 million. Under both the Rush and Boucher bills, social networking sites would also be required to obtain affirmative consent for the collection and disclosure of all, or substantially all, of an individual's online activity.

On July 27, 2010, in a Senate Commerce Committee "Consumer Online Privacy" hearing, Senator John Kerry (D-MA) announced plans to introduce legislation that would establish baseline online privacy protections for consumers.

The message regulators and legislators are sending to the private sector is this: if the private sector will not create a baseline for online privacy, Washington will legislate or regulate one.

The Facebook Five, Jail and Twitter: Social Media Networking and Litigation

Consistent with the effect that social networking websites are having on all areas of American life, social networking sites are having an impact on the legal system and the courtroom. Consider the following:

Twitter: Tweeting may land you in prison. In Los Angeles, a screenwriter was locked up after his alleged Twitter messages revealed he was in a furlough program instead of jail.[24] In Britain, a 26-year-old accountant was convicted of sending a menacing message after tweeting to his 600 Twitter followers that he would blow a local airport sky high.[25]

Facebook: Should a judge Facebook "friend" a witness in order to resolve a discovery dispute? In *Barnes v. CUS Nashville, LLC*, the plaintiff alleged injuries arising out of her fall one evening while dancing on top of a bar at the defendant's saloon. The defendant subpoenaed Facebook for the plaintiff's Facebook information, including photos of the plaintiff and her friends dancing on the bar. The court quashed the subpoena and in response, the defendant subpoenaed the plaintiff's friends, seeking photos posted by the plaintiff and her friends that depicted the events. The federal magistrate judge in Tennessee offered to create a Facebook account "for the sole purpose of reviewing photographs and related comments *in camera* . . . and disseminat[ing] any relevant information to the parties."[26] If the witnesses

accepted the judges Facebook "friend" requests, the judge agreed to review their Facebook information, provide any relevant information or photographs to the parties, and then close the Facebook account. To date, it appears neither party has taken Judge Brown up on his offer.

The Facebook activities of jurors in the recent criminal corruption trial of former Baltimore Mayor Shelia Dixon almost led to an overturned jury verdict. After a verdict had been entered for the prosecution, but before sentencing, defense attorneys discovered that five members of the jury had "friended" each other on Facebook and conducted private discussions about the case. Dixon entered into a plea agreement before the judge made any ruling regarding the jurors' improper communications.[27]

Once again, the use of technology is outpacing the law. Divorce lawyers routinely use social networking sites to gather evidence of infidelity. Libel attorneys use Twitter and Google to find evidence that belies libel plaintiffs' claims of damaged reputations and emotional distress. Trial attorneys routinely use Facebook and Google to investigate potential jurors during voir dire. Despite long-standing rules prohibiting jurors from discussing cases before them, jurors are blogging about their experiences. In 2009, defense lawyers in the federal corruption trial of former Pennsylvania State Senator Vincent J. Fumo demanded a mistrial when they discovered that a juror posted updates on the case on Twitter and Facebook.[28] The judge allowed deliberations to continue and the jury found Mr. Fumo guilty, but his lawyers plan to use the juror's Internet postings as grounds for appeal.

In 2009, the U.S. Judicial Conference on Court Administration and Case Management propounded new proposed jury instructions to govern jurors' use of social media during trials and jury deliberations.[29] The new instructions would prohibit jurors not only from using any form of electronic media to obtain information about a case, but also from using social networks – or any devices used to access social networks – to communicate about a case. Given how easy it is to access information and the resources required to enforce such a policy, however, enforcement will likely prove difficult.

For employees, online social networking poses its own legal risks. According to a 2009 study by Harris Interactive for CareerBuilder.com, 45 percent of employers questioned reported using social networks to screen job candidates, up from 22 percent a year earlier.[30] In the 2009 study, 35 percent of employers decided not to offer a job to a candidate based on information discovered on a social networking site. More than 50 percent of employers said that posting provocative photos or inappropriate information was the biggest factor in a decision not to hire an employee, while 44 percent cited references to drinking and drug use.[31] Recent high profile firings of media employees for content posted on social networking sites also illustrate the risk faced by employees.[32]

The risks associated are not limited to employees. Employers are turning increasingly to social networking as a tool to monitor employees' online behavior. But employers who use social networking sites as a way to monitor employee's off-duty conduct could run afoul of state privacy or whistle-blower statutes. In June 2009, for example, a federal jury in New Jersey found that managers for Hillstone Restaurant Group violated state and federal laws that protect the privacy of Web-based communications when they fired two employees who set up a private MySpace group to allow restaurant employees to "vent" about work.[33] Hillstone is appealing the verdict.

The Evolving Definition of Privacy

The notion of privacy has evolved rapidly over the past decade. The growth of social networks such as Facebook, Twitter, and Foursquare demonstrate that, with the right incentives, individuals are increasingly willing to disclose personal information.

Yet information shared online can have real "off-line" consequences. Banks and financial institutions are developing risk assessment algorithms based on an account applicant's online friends.[34] What is more, insurance companies may use information obtained through social networks to deny insurance benefits. In Canada, for example, a woman on sick leave for depression lost her insurance benefits after her insurer found Facebook photos of her on vacation, at a bar, and at a party.[35]

Despite these risks, interest in social networks is growing exponentially. The benefits of networking, sharing content, and connecting with friends and family members for free appear to outweigh user concerns about the disclosure of personal information.

Constance M. (Connie) Pendleton is a partner in Davis Wright Tremaine LLP's Washington, D.C. office, where she focuses her practice on media and first amendment issues, including privacy matters. Her clients include well-known cable networks, television and radio broadcasters, book, magazine, newspaper and online publishers, book sellers, journalists and authors. Connie can be reached at 202.973.4229 and conniependleton@dwt.com.

Erin Nedenia Reid is an associate in Davis Wright Tremaine LLP's Washington, D.C. office, where she specializes in media and communications matters. As a former law clerk with A&E Television Network and for FCC Commissioner Michael Copps, she has handled a variety of work related to communications, technology and privacy law. Erin can be reached at 202.973.4239 or erinreid@dwt.com.

---

[1] Alison Diana, *Social Media Up 230% Since 2007*, Information Week, June 28, 2010 (hereinafter "*Social Media Up 230% Since 2007*") (http://www.informationweek.com/news/software/web_services/showArticle.jhtml?articleID=225701600&subSection=News).

[2] *Id.*

[3] Experian Simmons, *2010 Social Networking Report*, at 4, June 10, 2010 (http://www.smrb.com/c/document_library/get_file?folderId=18244&name=DLFE-3601.pdf).

[4] Alison Diana, *Social Media Up 230% Since 2007.*

[5] Facebook, *Press Room Statistics* (http://www.facebook.com/press/info.php?statistics).

[6] Twitter Blog, *Measuring Tweets*, Twitter, Feb. 22, 2010 (http://blog.twitter.com/2010/02/measuring-tweets.html).

[7] The Official YouTube Blog, *At five years, two billion views per day and counting*, YouTube, May 16, 2010 (http://youtube-global.blogspot.com/2010/05/at-five-years-two-billion-views-per-day.html).

[8] Facebook, *Facebook's Privacy Policy* (http://www.facebook.com/policy.php).

[9] Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 194 (1890).

[10] *In Re Matter of Twitter*, Consent Order, FTC File No. 0923093, Federal Trade Commission (June 24, 2010) (hereinafter "*In Re Matter of Twitter* Consent Order"). (http://www.ftc.gov/os/caselist/0923093/100624twitteragree.pdf); *see also* Twitter Blog, *FTC Announcement* (http://blog.twitter.com/2010/06/ftc-announcement.html).

[11] *In Re Matter of Twitter*, Complaint, FTC File No. 0923093, Federal Trade Commission (http://www.ftc.gov/os/caselist/0923093/100624twittercmpt.pdf).

[12] *In Re Matter of Twitter* Consent Order at 6.

[13] *Id.* at 3-4.

[14] Electronic Privacy Information Center, Complaint, *In the Matter of Google, Inc.* at 4 (hereinafter "EPIC Complaint") (http://epic.org/privacy/ftc/googlebuzz/GoogleBuzz_Complaint.pdf).

[15] "*In re: Google Buzz Privacy Litigation,*" Case No. 5:10-cv-00672-JW (N.D. Cal. Feb. 17, 2010) (complaint). The complaint against Google alleged violations of the Electronic Communications Privacy Act, 18 U.S.C. §2510 *et seq.*, Stored Communications Act, 18 U.S.C. § 2701 *et seq.*, Computer Fraud and Abuse Act, 18 U.S.C. §1030 *et seq.*, California's Public Disclosure Tort, and California's Business and Professions Code (California's Unfair Competition Law) §17200.

[16] EPIC Complaint at 1.

[17] Cecilia Kang, *Privacy Advocates File FTC Complaint on Google Buzz*, Wash. Post online, Feb. 17, 2010 (http://voices.washingtonpost.com/posttech/2010/02/privacy_advocates_file_complai.html).

[18] Miguel Helft, *Anger Leads to Apology From Google About Buzz*, N.Y. Times, Feb. 15, 2010. (http://www.nytimes.com/2010/02/15/technology/internet/15google.html); *see also* Todd Jackson, *A new Buzz start-up experience based on your feedback*, The Official Gmail Blog, Feb. 13, 2010. (http://gmailblog.blogspot.com/2010/02/new-buzz-start-up-experience-based-on.html).

[19] David Kravets, *Facebook Denies 'All Wrongdoing' in 'Beacon' Data Breach*, Wired, Feb. 11, 2010 (http://www.wired.com/threatlevel/2010/02/facebook-denies-all-wrongdoing-in-beacon-data-breach/).

[20] Nancy Gohring, *Facebook Faces Class-Action Suit Over Beacon*, Network World, Aug. 13, 2008 (http://www.networkworld.com/news/2008/081308-facebook-faces-class-action-suit-over.html).

[21] Chloe Albanesius, *Facebook Partners With Nielsen, Ditches Beacon*, PCMag.com, Sept. 22, 2009 (http://www.pcmag.com/article2/0,2817,2353156,00.asp).

[22] Wendy Davis, *Facebook Sued Again Over Allegedly Leaking Information to Advertisers*, MediaPost, June 18, 2010 (http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=130530).

[23] Press Release, *FTC Seeks Comment on Children's Online Privacy Protections; Questions Whether Changes to Technology Warrant Changes to Agency Rule*, March 24, 2010 (http://www.ftc.gov/opa/2010/03/coppa.shtm).

[24] Raja Abdulrahim, *Tweeting Blows the Whistle on 'Pulp Fiction' co-screenwriter*, L.A. Times, Nov. 28, 2009 (http://articles.latimes.com/2009/nov/28/local/la-me-avary28-2009nov28).

[25] The Daily Mail, *Twitter User Paul Chambers Found Guilty After Threat to Blow Up Robin Hood Airport*, May 10, 2010 (http://www.dailymail.co.uk/news/article-1276394/Twitter-user-Paul-Chambers-guilty-threat-blow-Robin-Hood-airport.html)

[26] *Barnes v. CUS Nashville LLC*, Case No. 3:09-CV-00764 (M.D. Tenn., June 3, 2010) (order granting in part motion to compel).

[27] Julie Bykowicz, *5 Dixon Jurors Recalled As Witnesses*, Balt. Sun, Dec. 30, 2009 (http://www.baltimoresun.com/news/maryland/baltimore-city/bal-md.dixon30dec30,0,92298.story).

[28] John Schwartz, *As Jurors Turn to Web, Mistrials Are Popping Up*, N.Y. Times, Mar. 17, 2009 (http://www.nytimes.com/2009/03/18/us/18juries.html).

[29] Judicial Conference on Court Administration and Case Management, *Proposed Model Jury Instructions, The Use of Electronic Technology to Conduct Research on or Communicate about a Case*, Dec. 2009 (http://www.uscourts.gov/uscourts/News/2010/docs/DIR10-018-Attachment.pdf).

[30] Jenna Wortham, *More Employers Use Social Networks to Check Out Applicants*, N.Y. Times, Aug. 20, 2009 (http://bits.blogs.nytimes.com/2009/08/20/more-employers-use-social-networks-to-check-out-applicants/).

[31] Press Release, CareerBuilder.com, *Forty-five Percent of Employers Use Social Networking Sites to Research Job Candidates, CareerBuilder Survey Finds*, August 19, 2009 (http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr519&sd=8/19/2009&ed=12/31/2009&siteid=cbpr&sc_cmp1=cb_pr519_&cbRecursionCnt=2&cbsid=0a70c09ebbcb46029ba8bfd097d5fb15-332865007-R6-4)

[32] *See* Howard Kurtz, *Unfriendly Fire: The Angry Media*, The Washington Post, August 2, 2010 (http://www.washingtonpost.com/wp-dyn/content/article/2010/08/02/AR2010080201071.html); Richard Huff, *CNN fires Octavia Nasr for Twitter post praising Hezbollah terrorist, says credibility 'compromised,'* The New York Daily News, July 7, 2010 (http://www.nydailynews.com/news/national/2010/07/07/2010-07-07_cnn_fires_octavia_nasr_for_twitter_post_praising_hezbollah_terrorist_says_credib.html).

[33] *Pietrylo v. Hillstone Restaurant Group*, Case No. 2:06-cv-05754 (D.N.J. Jun. 16, 2009) (jury verdict).

[34] Erika Morphy, *Creepy Ways Your Social Media Data Can Be Used*, TechNewsWorld, Jan. 21, 2010 (http://www.technewsworld.com/story/69158.html?wlc=1279155768).

[35] Amy Luft, *Canada Woman to Fight Insurance Co. Over Facebook*, Seattle Times, Nov. 23, 2009 (http://seattletimes.nwsource.com/html/nationworld/2010336991_apcncanadafacebookinsurance.html?syndication=rss).