

# Privacy Expectations in Online Social Media—An Emerging Generational Divide?

STEVEN D. ZANSBERG AND JANNA K. FISCHER

Does one have a reasonable expectation of privacy in the contents of a postcard, discussing highly personal medical information that is dropped into a U.S. postal box for mailing? Years ago, this question was posed to attendees at the Media Law Resource Center's "London Conference" at Stationer's Hall. All of the American attorneys in the audience raised their hands expressing the belief that there is no such expectation of privacy in the postcard's contents because it was open to viewing by anyone who came in contact with it. In contrast, the European (indeed, all non-American) practitioners in attendance expressed their belief that the contents of the postcard enjoyed privacy protection because it contained highly personal and intimate information, not intended for a mass audience. This concrete example starkly demonstrates how different cultural norms shape the view of what is a reasonable expectation of privacy.

The postcard example was not a purely theoretical exercise; the point it illuminated is firmly grounded in American privacy law. After all, the Constitution prohibits the government from conducting an unreasonable search or seizure of information, which has been judicially limited to information as to which an individual has both a subjective expectation of privacy and an objectively reasonable one. In order for an expectation of privacy to be reasonable, it must "be one that society is prepared to recognize as 'reasonable.'" Similarly, for information to be subject to a privacy expectation that is protectable in civil tort law,<sup>2</sup> the defendant's intrusion

into one's sphere of personal privacy must be "a substantial one, of a kind that would be highly offensive to the ordinary reasonable [person],"<sup>3</sup> and must interfere with a privacy expectation that is objectively reasonable.<sup>4</sup> Expressly recognizing the degree to which such determinations are governed by the social norms of the relevant community, the Restatement declares that "[t]he protection afforded to the plaintiff's interest in his privacy must be relative to the customs of the time and place, to the occupation of the plaintiff and to the habits of his neighbors and fellow citizens."<sup>5</sup>

Precisely what type of privacy expectation society is prepared to recognize as reasonable varies not only by geography or nationality, as between individuals living in the United States and those living across the pond, but also by age. Today's younger users of social media (tweeters, bloggers, and other so-called netizens) have decidedly different notions of what it means to post information to limited or restricted communities using online social media platforms than do their older counterparts who may spend little, if any, time participating in such virtual communities. Yet, it is this older cohort who presently predominate the ranks of judges, the individuals who decide what types of information society as a whole is prepared to recognize and protect as private.<sup>6</sup>

This article examines how social norms, customs, and mores are evolving among users of online social media, and how those norms of what is a reasonable expectation of privacy may be in tension with the current view from the bench. One note up front: the authors do not offer a normative assessment (i.e., what the law should be), but only a more modest, descriptive analysis of the current state of the law as well as some predictions about where the law may be headed in the future.

## Tell One, Tell All

Although there are some exceptions, the prevailing view of information disclosure is as follows:

... a person cannot have a justifiable and constitutionally protected expectation that a person with whom he is conversing will not then or later reveal that conversation . . . Basically, the Supreme Court has recognized the simple fact that a thing remains secret until it is told to other ears, after which one cannot command its keeping. What was private is now on other lips and can no longer belong to the teller.<sup>7</sup>

As a related and logical extension of this conception of voluntary information disclosure as, essentially, a waiver of one's reasonable expectation of privacy, the courts have consistently held that "what a person knowingly *exposes to the public*, even in his home or office, is not subject to [constitutional] protection [as private information]."<sup>8</sup>

Of course, these doctrines are limited to information that is voluntarily disclosed by the person claiming a privacy interest in the information. In contrast, when a person's private information is obtained or disclosed without his or her consent, those rules are inapplicable.<sup>9</sup> It is also worth mentioning that what is a reasonable expectation of privacy may also depend on the context of the intrusion: criminal versus civil, government actors versus nongovernmental actors.<sup>10</sup>

As online social media use has grown, users have become more comfortable sharing their biographical information, photos, videos, personal hygiene habits, and other hobbies and interests publicly. Those of us with gray hair (or who once purchased 45-rpm singles) view those who regularly tweet, blog, and post personal photo albums as essentially treating their lives as an open book—exposing one's

---

*Steven D. Zansberg is a partner in the Denver office of Levine, Sullivan, Koch & Schulz, L.L.P. Janna Fischer, currently serving as a law clerk in that office, is a J.D. candidate (2012) at the University of Colorado School of Law.*

daily routines, and often including not only the mundane but also highly personal and intimate details, to public view.<sup>11</sup> In actuality, though, many online social media site users restrict at least some of the information they disclose to only their own contacts or “friends,” even if they also (must) assume that such information can be easily transmitted and disseminated outside that circle of invited guests,<sup>12</sup> and may also in many circumstances be accessed by complete strangers. Nevertheless, many such users demonstrate an expectation that the information they have posted will be “public” only within the circle of friends, no matter how large that circle may be. The question for the courts, and ultimately for society, is whether such an expectation is objectively reasonable.<sup>13</sup>

### What Is Public in Other Contexts?

Before the creation and proliferation of online social media platforms, the Supreme Court addressed whether people had a reasonable expectation of privacy in the phone numbers they dialed, which were necessarily and automatically exposed to the phone company, i.e., a third party, every time that they placed a call.<sup>14</sup> The police, acting without a search warrant, had attached a pen register to the suspect’s phone, which recorded all of the phone numbers that he dialed.<sup>15</sup> The suspect claimed that this was an unreasonable search in violation of his rights under the Fourth Amendment. The Supreme Court disagreed.<sup>16</sup> The suspect could not have had a reasonable expectation of privacy, the Court held, because he must have known that he was transmitting that information to the phone company every time he dialed a number.<sup>17</sup> “[E]ven if [the suspect] did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not ‘one that society is prepared to recognize as ‘reasonable.’”<sup>18</sup>

Importantly, the Court drew a distinction between an individual’s privacy expectation in phone numbers dialed with his privacy expectation in the contents of his phone conversations: “Although [the suspect’s] conduct may have been calculated to keep the *contents* of his conversation private, his *conduct* was not and could not have been calculated to preserve

the privacy of the number he dialed.”<sup>19</sup>

E-mails, like the phone numbers dialed (as opposed to the contents of phone conversations), are exposed to third parties because they are transmitted through an Internet service provider (ISP). However, in contrast to how courts have treated other open communications, multiple courts have held that the contents of e-mails are presumptively private.<sup>20</sup> In *United States v. Warshak*, the Sixth Circuit likened e-mail in the hands of one’s e-mail provider (or ISP) to traditional mail sent through the post office, where no user of the post office would reasonably expect a mail carrier to open his or her mail.<sup>21</sup> Similarly, the court reasoned that merely because the ISP could access e-mail at any time did not mean that the user reasonably expects the ISP to do so.<sup>22</sup> “[T]he mere *ability* of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy.”<sup>23</sup> Thus, the court concluded, e-mails are more like sealed envelopes than postcards whose contents are open for all to see.

Courts have consistently drawn a distinction between one’s privacy expectations in the contents of an e-mail message and in the transactional information (like a phone number dialed) that identifies a communication but that does not disclose its contents.<sup>24</sup> For example, the Ninth Circuit has said that e-mail users “have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.”<sup>25</sup> Information like an IP address or the addressee of an e-mail is considered to be the same as a dialed phone number that is automatically transmitted to the phone company.<sup>26</sup>

### Open Social Networking Sites

Turning away from transactional data that users necessarily transmit each time they access the Internet to the actual posting of content (text, photos, video, etc.), the courts have thus far analogized such publications to shouting from a rooftop or posting a sign on a kiosk in the town square. The basis for these rulings is the courts’

understanding of what users reasonably expect under the circumstances: any information users share with a social networking site has been provided to the site. This holds true even if users were to use the site’s privacy settings to hide the information from everyone but themselves.<sup>27</sup> The privacy policies of many social networking sites warn users that the very purpose of the site is to share information, and users should be aware that the public can see posts.<sup>28</sup> Because the Internet is

## Like all other written communications, postings and user profiles on social media sites are open to subpoena . . .

public and users by posting information have agreed to make the information public, courts tend to analogize social network postings to a bulletin board instead of a private e-mail.

To be sure, the body of case law in this area is still relatively sparse, and only a handful of courts have had occasion to grapple with the rapidly evolving nature of privacy settings and their implications for reasonable expectations of privacy. Two leading cases suggest that courts will view information posted on a publicly available social media site as not entitled to any privacy protection (regardless of how few people actually accessed the information) and may well treat as private information whose access is restricted to a class of people (not open to all) even if it is a large class.

In the first category, the California Court of Appeal held in *Moreno v. Hanford Sentinel* that a teenager’s poem posted to her MySpace page was not entitled to privacy and therefore a high school principal did not invade her privacy when he provided a copy of that poem to the town newspaper, which published it.<sup>29</sup> Although the student left the poem online only for a few days and intended only that a few people see it, the court ruled that her potential audience was “vast.”<sup>30</sup> “Under these circumstances, no reasonable person would have had an expectation of privacy regarding the

published material.”<sup>31</sup>

In the same vein, although from a very different vantage point, a Minnesota court held that a clinic worker’s posting to her MySpace page constituted sufficiently widespread publicity to make out a claim for publicity given to private facts (by the person whose private information was publicized), even though the posting was available online only for a few days.<sup>32</sup> The defendant, a worker at a medical clinic, upon seeing a relative come into the clinic for treatment, accessed the relative’s chart and learned that she had been treated for a sexually transmitted disease.<sup>33</sup> The worker created a MySpace page revealing the relative’s identity and that she had cheated on her husband.<sup>34</sup> Although possibly as few as six people had accessed the page, the court held that because the page was “available to the public at large,” it was sufficient to satisfy the widespread publicity element of the tort claim.<sup>35</sup> Thus, the patient, whose private information was posted to the public without her consent, had a valid privacy claim against the clinic worker for the MySpace posting.

### Social Media Sites and Civil Discovery

Like all other written communications, postings and user profiles on social media sites are discoverable and subject to subpoena, as long as the subpoena or discovery request is not overly broad and the information sought is relevant to the matters being litigated. In resolving civil discovery disputes, several courts have reached the same conclusion as the court in *Moreno*, that information that is available to all on the Internet, even if it was subjectively intended only to be seen by a limited audience, is not entitled to a reasonable expectation of privacy.<sup>36</sup> The more intriguing question is whether users can maintain a reasonable expectation of privacy when they post information to a social media website that is not available to everyone but is restricted to a defined and delimited group of friends or contacts.

In *Romano v. Steelcase*,<sup>37</sup> the court granted a defendant’s motion for access to the private portions of a personal injury plaintiff’s Facebook and MySpace pages because the publicly available portions showed her as active and apparently healthy; therefore, the

defendant claimed, the private portions of her social network pages were likely to include other relevant information.<sup>38</sup> Notably, the court held that the plaintiff had no reasonable expectation of privacy in her social network postings, including those restricted to certain colleagues or acquaintances, because the sites’ “very nature and purpose” was to share information with others.<sup>39</sup> She consented to share her personal information with others, notwithstanding her privacy settings that limited who she authorized to view her information: “Since Plaintiff knew that her information may become publicly available, she cannot now claim that she had a reasonable expectation of privacy.”<sup>40</sup> Quoting a law review article, the court stated: “In this environment, privacy is no longer grounded in reasonable expectations, but rather in some theoretical protocol better known as wishful thinking.”<sup>41</sup>

In contrast to the ruling in *Romano*, a federal district court in California has held that information posted online that is shared only with a limited group (even a potentially large one) is entitled to privacy and therefore not discoverable though a civil subpoena under the Stored Communications Act (SCA), 18 U.S.C. §§ 2701 et seq. In *Crispin v. Christian Audigier, Inc.*,<sup>42</sup> a clothing designer sued a clothing manufacturer over the use of designs without attribution. In discovery, the defendant manufacturer sought, via a subpoena on the plaintiff’s ISP, all of the designer’s communications through social networking sites, including those he had restricted only to his friends by using the site’s settings restricting access. The court remanded to the trial court to determine whether the evidence showed the plaintiff’s postings to Facebook and MySpace were in fact not available to the general public but instead restricted to identified individuals. If so, the court held the postings would be private communications, which are not discoverable though a civil subpoena under the SCA.<sup>43</sup> If, on remand, the postings were found to be restricted to only certain friends of the plaintiff, they would be functionally equivalent to e-mails, despite their being “available to hundreds or thousands of approved users.”<sup>44</sup>

The court in *Romano* took the view that anything posted online was public

(i.e., no longer private) because of the potential for anyone to see it (ostensibly through reposting by someone with access rights), even if the user had restricted the information to a select group of people. The *Crispin* court took a very different view of one’s privacy expectation in information shared only with a select group of individuals, even if that group is quite large (e.g., thousands of approved recipients).

### Limited Information Disclosure

Many, perhaps even the majority, of users of social networks consider their information open only to those within their circle of contacts, no matter how large that circle may be.<sup>45</sup> The way people use social networks, i.e., assuming that the information that they post will be seen only by those to whom they have given permission, comports more with cases where courts have found a reasonable expectation of privacy in information that someone shared only with a limited group of intimates, not in a public setting.

Even before the advent of the Internet, a few courts recognized that, in certain circumstances, disclosure of information to a limited group of people (even absent any contractual or other legal duty that they maintain its confidentiality) does not forfeit one’s reasonable expectation of privacy in such information. For example, in *Times Mirror Co. v. Superior Court of San Diego*,<sup>46</sup> the California Court of Appeal found actionable as a publication of private facts a newspaper’s publication of the name of a witness to a crime (before the murderer had been apprehended), notwithstanding the fact that the plaintiff had disclosed that information to “certain friends, neighbors, and family members.” The court determined that her identity as the person who had discovered the body and identified the murderer was not thereby rendered public information: “Talking to selected individuals does not render private information public. . . . On the record before us we cannot say Doe rendered otherwise private information public by cooperating in the criminal investigation and seeking solace from friends and relatives.”<sup>47</sup>

The California Court of Appeal again recognized a continuing privacy interest, even following disclosure of information to a select group of family

and friends, when it held actionable an invasion of privacy claim by children on a Little League team whose photo was published by *Sports Illustrated* in connection with a story about Little League coaches and managers who molest children.<sup>48</sup> The court stated that “the claim of the right of privacy is not ‘so much one of total secrecy as it is the right to define one’s circle of intimacy—to choose who shall see beneath the quotidian mask.’”<sup>49</sup> Even though the photograph at issue had been distributed among family members of the Little League players, the court held that the “photograph was intended to be private, only for dissemination among family and friends.”<sup>50</sup>

California’s Supreme Court adopted the same view with respect to information that is disclosed to some, but not to the general public, in *Sanders v. American Broadcasting Co.*:

Privacy, for purposes of the intrusion tort, is not a binary, all-or-nothing characteristic. There are degrees and nuances to societal recognition of our expectations of privacy: the fact that the privacy one expects in a given setting is not complete or absolute does not render the expectation unreasonable as a matter of law.<sup>51</sup>

Notably, however, none of these cases involved information that was held open for viewing by the general public. Indeed, the decision in *Sanders*, which involved a TV news crew’s surreptitious videotaping of conversations between workers in an office setting, expressly distinguished other cases on grounds that “[a]s the briefed question is framed, the interactions at issue here could *not* have been witnessed by the *general public*.”<sup>52</sup>

The case law is consistent with the view of the Restatement of Torts, which recognizes that privacy of certain information may be maintained so long as the individual “does not expose [that information] to the public eye, but keeps [it] entirely to himself or at most reveals [it] *only to his family or to close personal friends*”; the Restatement further makes clear that “there is no liability for giving . . . publicity to what the plaintiff himself *leaves open* to the public eye.”<sup>53</sup> What the age of online social media calls into question is what this comment means when it

mentions “close personal friends.” For example, in the wake of his infamous public meltdown, television star Charlie Sheen began tweeting to more than two million of his Twitter followers as well as making his tweets publicly available. Even if he had restricted his tweets to be visible only to his followers, that would be a fairly sizeable collection of close personal friends.

As the postcard example demonstrates, the means by which information is transmitted to others can be determinative of its status in the privacy analysis. There is a pivotal difference between sending e-mail or text messages to one or several recipients (any one of whom could, lawfully, thereafter forward that information on to others or post it publicly online) and sending information to one’s followers via a website like Twitter, which may be accessible to anyone (if not restricted only to one’s followers).<sup>54</sup>

#### Password-Protected Networks

When information is only accessible to a closed group of subscribers, some courts have held that it is entitled to a reasonable expectation of privacy. For example, in *Pietrylo v. Hillstone Restaurant Group*, information posted on a restaurant’s employee-only social media site was held to be nonpublic, and a manager’s access to that closed site was deemed unauthorized when the manager pressured an employee to give him the password.<sup>55</sup> The site in question was an employee-created chat group on MySpace.com, accessed by invitation and then the members’ MySpace accounts and passwords, to which the creator had restricted access.<sup>56</sup> The court sustained the jury’s finding that the restaurant manager’s repeated access to the site violated the SCA because the employee who provided the manager her password did so under a perceived threat to her employment, and thus her “purported ‘authorization’ was coerced or provided under pressure.”<sup>57</sup> The website’s contents made clear that “it was intended to be private and only accessible to invited members.”<sup>58</sup> Notably, though, the jury returned a defense verdict on the plaintiffs’ common law invasion-of-privacy claim, which was not the subject of a post-trial motion.<sup>59</sup>

A similar employee-only restricted website was held to be private in *Konop v. Hawaiian Airlines, Inc.*, where the

website’s creator, a commercial airline pilot, had restricted access to a list of employees.<sup>60</sup> Konop had restricted access to his website exclusively to fellow Hawaiian Airline pilots but permitted them to create their own passwords.<sup>61</sup> Two pilots had given a manager permission to create passwords using their names, and the Ninth Circuit held that the manager’s access was unauthorized (in violation of the SCA) because they had never used the site themselves and were therefore not users who could

## ... there is a difference between the privacy expectations of “digital natives” . . . and those of “digital immigrants” . . .

authorize the manager’s access.<sup>62</sup> Because Konop had plainly intended to restrict his website to a list of authorized users, he had an expectation that the posts on his website would remain within that group of users and not accessed by uninvited visitors.<sup>63</sup>

#### What Does Age Have to Do with It?

Both *Pietrylo* and *Konop* involved limited-access discussion boards that provided access only to certain identified authorized users. In contrast, social network sites like Facebook are accessible to much broader audiences. Despite these rather stark factual distinctions, many social network users, particularly those of certain generations, expect that their information will remain within the network and not be seen by the vast potential audience, as the court in *Moreno* described it.

According to surveys, a majority of social network users take advantage of the networks’ privacy settings and, based upon those settings, believe that they have some privacy online.<sup>64</sup> A 2009 study of college students at the University of Miami in Florida and Ryerson University in Canada showed that most of these students thought it was wrong for someone to whom they did not give permission to access their social media pages.<sup>65</sup> A majority of these

students believed that they had taken appropriate steps to keep their information within their own set of friends or contacts.<sup>66</sup> The survey's authors described the students as "technologically savvy, yet somewhat dismissive of potential risks online."<sup>67</sup> The authors of that study formulate "a notion of privacy based on the expected accessibility of personal information to social constituencies."<sup>68</sup>

The results of the 2009 survey led another author, Bryce Clayton Newell, to argue that even though social network users posted information on the Internet, and by doing so apparently expressed a desire to share that information with the general public, their use of network privacy settings to restrict access of their information only to their "contacts" demonstrated that the users did not intend the information to be fully public. Thus, they maintained a reasonable expectation of privacy in such information, despite sharing it with a large group of selected individuals. Accordingly, Newell advocates, courts should not treat the information as public.<sup>69</sup>

Notably, Newell says that there is a difference between the privacy expectations of "digital immigrants," defined as those who did not grow up using Facebook, and those of "digital natives," i.e., young people like the subjects of the 2009 study, who did.<sup>70</sup> While the former treat the Internet as public, the latter retain an expectation that what they post will and should remain among the people they choose to see it.<sup>71</sup> Other commentators, recognizing this growing community view (in other words, the social norm) concerning limited information disclosure, even on publicly available media, have advocated for a change in the law, to recognize and embrace what this segment of society is willing to recognize as a reasonable expectation of privacy.<sup>72</sup>

As further support for this sub-cultural view of limited information disclosure (i.e., rather than a binary choice between complete secrecy and no privacy), several privacy breaches involving social networks or similar websites and the resulting outcry clearly demonstrate the expectation of users that certain information they share with a social media website will remain only within their circle of friends.

### Social Media Faux Pax

Three incidents and the public reaction to them illustrate that social media site users actually do expect that their information will remain within their social network, at least if the user has not affirmatively consented to its release or disclosure. Users reacted poorly to Facebook's launch of its Beacon feature, which lifted data from external websites to Facebook users' feeds; to the hacking of Twitter, resulting in a potential privacy breach; and to Google's launch of the Buzz feature, which created a Facebook-like interface within its e-mail system and made all its users' contacts visible to each other.

Facebook's 2007 launch of its Beacon feature, which sent data from external advertisers' sites to Facebook so that Facebook users could share their purchases with their contacts, sparked an immediate user outcry.<sup>73</sup> The feature fed information about users' purchases into their news feeds, the list of actions Facebook users see about their friends when they log into the site. Beacon let users know when someone they knew had made a purchase and what that purchase was (in some cases, spoiling surprise Christmas gifts).<sup>74</sup> Beacon transmitted data about purchases to Facebook even when a user opted out of having the purchase displayed in his feed, which was of particular concern to social-network watchers.<sup>75</sup>

Upset Facebook users filed a class action lawsuit over Beacon, which was settled in February 2010.<sup>76</sup> Facebook terminated Beacon in November 2009, although the site continued to collect information from third-party advertisers unless the user had opted out of the setting.<sup>77</sup> Users filed a new class action lawsuit over this feature, alleging violations of the Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2510 et seq.; the SCA; and California law.<sup>78</sup> In May 2011, the district court granted Facebook's motion to dismiss these claims.<sup>79</sup> Facebook did not violate the ECPA, the court held, because, as a lawful recipient of the communications, it had permission to divulge them.<sup>80</sup> Facebook did not violate the SCA, the court held, because the plaintiffs sent their information either to Facebook or directly to an advertiser by clicking on a banner ad, and in either case Facebook or the

advertiser had lawfully received the communication.<sup>81</sup>

In January and again in April 2009, the networking site Twitter was hacked by intruders who gained access through Twitter employees' logins.<sup>82</sup> The hackers sent fake tweets from accounts, including those of Fox News and President Barack Obama.<sup>83</sup> The FTC filed a formal complaint alleging that Twitter violated the Federal Trade Commission Act, 15 U.S.C. §§ 41–58, by representing that it "used reasonable and appropriate security measures to honor the privacy choices exercised by users" when it did not.<sup>84</sup> Twitter allowed employees to use their personal e-mail accounts to access Twitter's administrative functions and did not have password strength requirements, thereby allowing hackers to gain access by using a random-password generator.<sup>85</sup> The FTC said that because Twitter did not take appropriate security measures but represented that it did, Twitter had engaged in deceptive trade practices.<sup>86</sup> The FTC and Twitter entered into a consent order that became final on March 2, 2011, barring Twitter for twenty years from misleading consumers about its security measures and ordering Twitter to honor the privacy choices expressed by Twitter users.<sup>87</sup>

In February 2010, the search engine Google, in an effort to compete with social media sites like Facebook, launched Google Buzz, a social networking engine within its Gmail e-mailing system, which allowed users to post social updates to their existing e-mail contacts.<sup>88</sup> Users complained about the automatic opt-in nature of Google Buzz, which made all of their contacts visible to each other, including highly personal contacts, such as doctors and attorneys, whom users might not have wanted their entire e-mail address book to see.<sup>89</sup> One blogger found herself being followed on Google Buzz by her abusive ex-husband, who was one of her e-mail contacts.<sup>90</sup> She strongly objected to him automatically seeing her recent comments on other posts and especially her location because she did not want him to be able to track her movements.<sup>91</sup> The Electronic Privacy Information Center (EPIC) filed a complaint with the FTC against Google alleging "clear

harms” to service subscribers, including the disclosure of “deeply personal information” such as which contacts users e-mailed most often.<sup>92</sup>

Google almost immediately backed off on Buzz’s so-called auto-follow feature and apologized to its users.<sup>93</sup> The FTC charged Google with deceptive practices in its rollout of Buzz, and Google and the FTC entered a settlement agreement in March 2011.<sup>94</sup> Under the agreement, approved October 11, 2011, Google will have to implement a comprehensive privacy program and undergo regular FTC audits for the next twenty years.<sup>95</sup>

These three recent incidents all show that even when users willingly share their information with social networking sites, they want that information to be secure and expect that the information will only be shared with people the users choose. Notably, the Google Buzz outcry shows that this expectation extends to items such as e-mail addresses in which several courts have found no reasonable expectation of privacy.<sup>96</sup>

#### Before You Click “Send”

Many users’ subjective expectation of privacy in information they post to a social media site does not necessarily coincide with courts’ views that such information is entitled to no reasonable expectation of privacy because it is either available to the public or shared with a sufficiently large group. At present, the traditional view—that information available to all (even if only actually viewed by a limited group) or shared with a sufficiently large group is entitled to no expectation of privacy that “society is prepared to recognize as reasonable”—prevails.

As we said at the outset, we do not offer a prescription for where the law governing privacy expectations on social networking sites should evolve, or even whether any further evolution is appropriate. However, it appears there may well be further evolution of the legal doctrine of information disclosure away from a binary, all-or-nothing, approach toward a more nuanced view of “limited information disclosure” that is dependent, in large part, on the privacy setting of various social networking sites (which themselves continue to evolve rapidly),<sup>97</sup>

and, perhaps, the size of the group that is given access to the information. There may well be a shift to accepting a more limited expectation of privacy in partial disclosure of information to a select group of recipients, not limited to one’s close personal friends. This shift is all the more likely to occur at some point in the not-too-distant future, when more judicial robes are donned by digital natives.

#### Endnotes

1. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). Most recently, the Supreme Court assumed, for purposes of resolving the case before it, that there is a constitutional right to informational privacy. *NASA v. Nelson*, 131 S. Ct. 746, 756 (2011); *but see id.* at 764 (Scalia, J., concurring) (“A federal constitutional right to ‘informational privacy’ does not exist.”); *id.* at 769 (Thomas, J., concurring) (“I agree with Justice Scalia that the Constitution does not protect a right to informational privacy.”). As others have noted, because judicial opinions declaring what society recognizes as reasonable have the effect of altering preexisting social norms, there is an inherent circularity at play as the law evolves. *See, e.g., Jed Rubenfeld, The End of Privacy*, 61 *STANFORD L. REV.* 101, 106 & n.23 (2008) (“Commentators have long condemned the ‘reasonable expectation of privacy’ as ineluctably circular.”) (citations omitted).

2. The courts do not always equate a reasonable expectation of privacy against governmental intrusion (protected by the Fourth Amendment) with a reasonable expectation of privacy against private intrusion for purposes of civil tort law or civil discovery. *See, e.g., Sanders v. Am. Broad. Co.*, 978 P.2d 67, 74 n.3 (Cal. 1999) (“decisions discussing . . . expectations of privacy against government searches are not directly applicable to the common law privacy tort context”). At least theoretically (and prospectively, from the vantage point of the speaker), it is difficult to see how one’s objectively reasonable expectation that a particular communication will not be intercepted or seized would vary depending on whether the intruder is enshrouded with governmental authority or a private actor. *See, e.g., Desnick v. Am. Broad. Co.*, 44 F.3d 1345, 1353 (7th Cir. 1995) (plaintiff could have no different reasonable expectation of privacy against alleged intrusion by undercover government testers than by undercover news reporters).

3. *RESTATEMENT (SECOND) OF TORTS*

§ 652B cmt. d (1977); *id.* § 652D cmt. c.

4. *See id.* § 652B cmt. c.

5. *Id.*; *see also* J. THOMAS MCCARTHY, *RIGHTS OF PUBLICITY AND PRIVACY* § 5:98 (2d ed. 2010) (recognizing that the zone of privacy “that is legally protected is dependent upon both the social customs and norms which govern a given context”) (citing Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 *CAL. L. REV.* 957 (1989)).

6. *See, e.g., United States v. Garzon*, 119 F.3d 1446, 1449 (10th Cir. 1997) (whether a person had “an objectively reasonable expectation of privacy . . . that society will recognize is a question of law that we review de novo”) (citation omitted); *but see Schulman v. Group W Prods., Inc.*, 955 P.2d 469, 490–91 (Cal. 1998) (holding that whether plaintiff had objectively reasonable expectation of privacy in conversations presents a jury question).

7. *Commonwealth v. Blystone*, 549 A.2d 81, 87 (Pa. 1988), *aff’d sub nom. Blystone v. Pennsylvania*, 494 U.S. 299 (1990) (citation omitted); *see also Alivoni v. Worcester Sch. Comm.*, 777 F.2d 776, 783–85 (1st Cir. 1985) (same); *United States v. Jacobsen*, 466 U.S. 109, 117 (1984) (“It is well settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities.”); *Larson v. Harrington*, 11 F. Supp. 2d 1198, 1202 (E.D. Cal. 1998) (“Harrington . . . has no objectively reasonable expectation of privacy in matter he previously discussed with co-workers.”). For a compelling argument that this voluntary waiver concept essentially guts the Fourth Amendment, *see Rubenfeld, supra* note 1, at 113–15.

8. *Katz v. United States*, 389 U.S. 347, 351 (1967); *see also Smith v. Maryland*, 442 U.S. 735, 743–44 (1979) (“This court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.”) (citations omitted).

9. *See RESTATEMENT (SECOND) OF TORTS* § 652D cmt. b (recognizing invasion of privacy when private photo of plaintiff is “stolen from his home . . . [and] made public when the picture appears in the newspaper”).

10. *See supra* note 2.

11. *See* Victor Keegan, *Where Does Privacy Fit on the Online Video Revolution?*, *GUARDIAN*, Mar. 19, 2010 (“Whatever our fears about governments collecting data about ourselves, we seem to be two steps ahead of them in revealing it all ourselves voluntarily.”); Mathew Ingram, *Yes Virginia*,

*Big Brother Is Following You on Twitter*, GIGAOM.COM (Aug. 16, 2011, 3 p.m.), <http://gigaom.com/2011/08/16/yes-virginia-big-brother-is-following-you-on-twitter/> (noting that “the New York Police Department has launched an official social media monitoring branch, whose job it will be to track Twitter and Facebook for information” and concluding that “[i]n a world where our online activities are increasingly public, . . . governments have even more ability to observe our behavior, whether we like it or not.”); Alex Kozminski & Stephanie Grace, *Pulling the Plug on Privacy: How Technology Helped Make the 4th Amendment Obsolete*, THE DAILY, June 22, 2011 (because “we don’t have reasonable expectations of privacy in things we’ve revealed to other people of the public,” and as a result of our willingness to voluntarily reveal information to third-party vendors in exchange for convenience and other incentives, “the Fourth Amendment is all but obsolete”).

12. Avner Levin & Patricia Sánchez Abril, *Two Notions of Privacy Online*, 11 VAND. J. ENT. & TECH. L. 1001, 1033 (2009).

13. See James Grimmelman, *Privacy as Product Safety*, 19 WIDENER L.J. 793, 798 (2010) (“Actual Facebook users act in ways that indicate that they very much care about privacy.”).

14. *Smith v. Maryland*, 442 U.S. 735, 740 (1979).

15. *Id.* at 737.

16. *Id.* at 742.

17. *Id.*

18. *Id.* at 743.

19. *Id.* (emphasis in original).

20. *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010); see also *United States v. Lucas*, 640 F.3d 168, 178 (6th Cir. 2011) (“We recognize individuals have a reasonable expectation of privacy in the content of emails stored, sent, or received through a commercial Internet service provider.”); *United States v. Long*, 64 M.J. 57, 64 (C.A.A.F. 2006) (servicemember’s “subjective expectation of privacy in [her] e-mails is one that society is prepared to accept as reasonable”).

21. *Warshak*, 631 F.3d at 285.

22. *Id.*

23. *Id.* at 286 (emphasis in original).

24. “The *Smith* line of cases has led federal courts to uniformly conclude that Internet users have no reasonable expectation of privacy in their subscriber information, the length of their stored files, and other noncontent data to which service providers must have access.” *United States v. D’Andrea*, 497 F. Supp. 2d 117, 120 (D.

Mass. 2007), *vacated on other grounds*, No. 08-2455, 2011 WL 1760207 (1st Cir. May 10, 2011).

25. *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008); accord *United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010), *cert. denied*, 131 S. Ct. 1513 (2011) (“[N]o reasonable expectation of privacy exists in an IP address, because that information is also conveyed to and, indeed, from third parties, including ISPs.”); *United States v. Hambric*, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999) (no reasonable expectation of privacy in one’s IP address).

26. *Forrester*, 512 F.3d at 510.

27. See *Privacy Policy*, FACEBOOK.COM, [www.facebook.com/policy.php](http://www.facebook.com/policy.php) (last visited Aug. 25, 2011) (detailing “Information You Provide to Us,” including IP address and site activity information in addition to any photos and personal information the user inputs on Facebook); *Twitter Privacy Policy*, TWITTER.COM, [twitter.com/privacy](http://twitter.com/privacy) (last visited Aug. 25, 2011) (Twitter saves information in addition to the contents of the user’s tweets, including location information).

28. *Twitter Privacy Policy*, *supra* note 27 (“Our Services are primarily designed to help you share information with the world.”); *Facebook Privacy Policy*, *supra* note 27 (“One of the primary reasons people use Facebook is to share content with others.”).

29. The teenager sued the principal for “public disclosure of private facts” because she intended that only her MySpace friends see her poem and the principal disclosed it to the town at large. *Moreno v. Hanford Sentinel, Inc.*, 91 Cal. Rptr. 3d 858, 862 (Ct. App. 2009).

30. *Id.* at 862–63.

31. *Id.* at 862.

32. *Yath v. Fairview Clinics, N.P.*, 767 N.W.2d 34, 43 (Minn. Ct. App. 2009). Cf. *Religious Tech Ctr. v. Lerma*, 908 F. Supp. 1362, 1368 (E.D. Va. 1995) (“Once a trade secret is posted on the Internet, it is effectively part of the public domain, impossible to retrieve.”); *Religious Tech. Ctr. v. Netcom On-Line Comm’n Servs., Inc.*, 923 F. Supp. 1231, 1256 (N.D. Cal. 1995) (once information becomes available to be accessed online, it is no longer secret); but see *DVD Copy Control Ass’n, Inc. v. Bunner*, 116 Cal. App. 4th 241, 251 (Cal. Ct. App. 2004) (“[p]ublication on the Internet does not necessarily destroy the secret if the publication is sufficiently obscure or transient or otherwise limited so that it does not become generally known”).

33. *Yath*, 767 N.W.2d at 39.

34. *Id.*

35. *Id.* at 43.

36. See e.g., *Zimmerman v. Weis Markets, Inc.*, No. CV-09-1535, slip op. at 6 (Northumberland Cnty. Ct. (Pa.), May 19, 2011) (a personal injury plaintiff’s publicly available photos showing him wearing shorts were relevant when his claim stated he could no longer wear shorts because of his scars); *Dexter v. Dexter*, No. 2006-P-0051, 2007 WL 1532084 (Ohio Ct. App. 2007) (no reasonable expectation of privacy in postings to MySpace public site); *Beye v. Horizon Blue Cross Blue Shield of New Jersey*, No. 06-5337 (FSH), 2007 WL 7393489 (D.N.J. Dec. 14, 2007).

37. 907 N.Y.S.2d 650, 656 (Sup. Ct. 2009).

38. *Id.*

39. *Id.* at 657.

40. *Id.*

41. *Id.* at \*6 & n.9 (quoting Dana L. Flemming & Joseph M. Herlihy, *Department: Heads Up: What Happens When the College Rumor Mill Goes Online? Privacy, Defamation, and Online Social Networking Sites*, 53 BOSTON B.J. 16 (2009)).

42. 717 F. Supp. 2d 965, 968 (C.D. Cal. 2010).

43. *Id.* at 990–91.

44. *Id.* at 990.

45. See Levin & Abril, *supra* note 12 (students at two colleges surveyed by the authors expressed the expectation that the information they posted was private within their own social network); Bryce Clayton Newell, *Rethinking Reasonable Expectations of Privacy in Online Social Networks*, 17 RICH. J.L. & TECH. 12 (2011) (users view their information as deserving some sort of privacy protection, even when their number of friends is high).

46. 198 Cal. App. 3d 1420 (1988).

47. *Id.* at 1428.

48. *M.G. v. Time Warner*, 89 Cal. App. 4th 623 (Cal. Ct. App. 2001).

49. *Id.* at 633.

50. *Id.* See also *Multimedia WMAZ, Inc. v. Kubach*, 443 S.E.2d 491, 494 & n.1 (Ga. Ct. App. 1994) (holding that plaintiff did not abandon his reasonable expectation of privacy in the fact of his HIV-positive diagnosis when he shared that information “with approximately 60 individuals” whom “he thought had reason to know of his disease”).

51. *Sanders v. Am. Broad. Co.*, 978 P.2d 67, 72 (Cal. 1999).

52. *Id.* at 77 (emphasis added); see also

Schulman v. Group W Prods., Inc., 955 P.2d 469, 491 (Cal. 1998) (finding triable issue on plaintiff's reasonable expectation of privacy in her conversation with the rescue crew at the accident scene, where records was unclear "whether passersby on the road could have heard [her] conversation").

53. RESTATEMENT (SECOND) OF TORTS § 652D cmt. b (1977); see also McCARTHY, *supra* note 5, § 5:93 ("If the plaintiff has already exposed the matter to wide public attention, he cannot thereafter claim that further exposure constitutes an invasion of privacy by 'intrusion.'") (citation omitted).

54. Compare former Congressman Anthony Weiner's tweets of images of his (now no longer) private parts with sexually explicit text messages exchanged between public officials over a government-funded server (held private, not public records). See *Denver Publ'g Co. v. Bd. of Cnty. Comm'rs of Cnty. of Arapahoe*, 121 P.3d 190 (Colo. 2005) (sexually explicit text messages bore no "demonstrable connection" to public officials' performance of public functions and were therefore not "public records" under Colorado's Open Records Act; statutory definition inherently protects "privacy interests of public employees").

55. CIV. 06-5754(FSH), 2009 WL 3128420, at \*3 (D.N.J. Sept. 25, 2009).

56. *Id.*

57. *Id.*

58. *Id.*

59. *Id.* at \*1 n.1.

60. 302 F.3d 868, 880 (9th Cir. 2002).

61. *Id.* at 873.

62. *Id.* at 880.

63. *Id.* Arguably, however, under the court's narrow holding, Konop would have no SCA claim if an authorized *user* of his website had authorized the Hawaiian Airlines manager to use that pilot's name to access the website. Distinguishing *Konop*, the Eleventh Circuit held that the SCA was not violated by the allegedly unauthorized access to an online bulletin board that merely required any visitor to register, ignore a warning, and falsely represent (through click-through assent) the lack of affiliation with a particular company. *Snow v. DirecTV*, 450 F.3d 1314, 1321–22 (11th Cir. 2006) ("In order to be protected by the SCA, an Internet website must be configured in some way so as to limit ready access by the general public.").

64. Woodrow Hartzog, *Promises and Privacy: Promissory Estoppel and Confidential Disclosure in Online Communities*, 82 TEMPLE L. REV. 891, 893 (2009) ("It is

far too facile, however, to conclude that because people are sharing private data online, they should expect no privacy. Many online communities have elaborate privacy settings."); Levin & Abril, *supra* note 12, at 1033; Newell, *supra* note 45, at \*3.

65. Levin & Abril, *supra* note 12, at 1027.

66. *Id.* at 1033 (72 percent of the surveyed students restricted their privacy settings and 54 percent blocked specific people from accessing their profile; 61 percent "believe they take the appropriate steps to limit access to their profiles.").

67. *Id.*

68. *Id.* at 1045.

69. Newell, *supra* note 45, at \*18.

70. *Id.* at \*19.

71. *Id.* ("to simply place all things Internet into a basket reserved for only completely public information would seriously undermine the actual subjective—and arguably reasonable—expectations of a large and growing segment of society"). See also McCARTHY, *supra* note 5, § 5:97 ("Even when one is in a public place, there can in some rare circumstances be something still protected as 'private' . . . What should be regarded as 'private' even though it occurs in public can change over time with changes in public attitudes.").

72. See, e.g., Newell, *supra* note 45; Hartzog, *supra* note 64; see also Robert Sprague, *Rethinking Information Privacy in an Age of Online Transparency*, 25 HOFSTRA LAB. & EMP. L. J. 395, 408–09 (2008) ("This all-or-nothing approach to privacy may be outmoded. . . . [Protecting legitimate user expectations] requires an attitudinal shift towards acceptance of the idea that just because a few people have access to information does not mean it is no longer private. . . . Just because we share confidential information with someone does not mean it is automatically 'public' (i.e., no longer private).").

73. See *Petition to Facebook*, MOVEON.ORG, <http://civ.moveon.org/facebookprivacy/071120email.html> (last visited Aug. 25, 2011) (calling on MoveOn members to tell Facebook to dismantle Beacon and containing comments from users upset that Beacon revealed their purchases); Juan Carlos Perez, *Facebook's Beacon More Intrusive Than Previously Thought*, PC WORLD (Nov. 30, 2007, 5:10 p.m.), [www.pcworld.com/article/140182/facebooks\\_beacon\\_more\\_intrusive\\_than\\_previously\\_thought.html](http://www.pcworld.com/article/140182/facebooks_beacon_more_intrusive_than_previously_thought.html); Om Malik, *Is Facebook Beacon a Privacy Nightmare?*, GIGAOM (Nov. 6, 2007, 4:19 p.m.), <http://gigaom.com/2007/11/06/>

[facebook-beacon-privacy-issues/](http://facebook-beacon-privacy-issues/) (calling Beacon a "privacy disaster waiting to happen").

74. Sean Lane's wife found out via Beacon about a jewelry purchase that Lane intended to be a surprise: "Sean Lane bought 14k White Gold 1/5 ct Diamond Eternity Flower Ring from overstock.com" was announced to all of his Facebook friends, including his wife. David Kravets, *Facebook Denies "All Wrongdoing" in "Beacon" Data Breach*, WIRED.COM (Feb. 11, 2010, 5:20 p.m.), [www.wired.com/threatlevel/2010/02/facebook-denies-all-wrongdoing-in-beacon-data-breach](http://www.wired.com/threatlevel/2010/02/facebook-denies-all-wrongdoing-in-beacon-data-breach).

75. See Malik, *supra* note 73; Perez, *supra* note 73.

76. Kravets, *supra* note 74.

77. *Id.* For Facebook's current "instant personalization" feature, see *Information You Share with Third Parties*, FACEBOOK.COM, [www.facebook.com/policy.php](http://www.facebook.com/policy.php) (last visited Aug. 25, 2011) ("You can disable instant personalization on all pre-approved websites and applications using your Applications and Websites privacy setting. You can also block a particular pre-approved website or application by clicking 'No Thanks' in the blue bar when you visit that application or website.").

78. *In re Facebook Privacy Litig.*, No. C 10-02389 JW, 2011 WL 2039995, at \*1 (N.D. Cal. May 12, 2011).

79. *Id.* at \*10.

80. *Id.* at \*6.

81. *Id.*

82. *In re Twitter, Inc.*, Dkt. No. C-4316, 092-3093 (FTC 2010) (complaint) *available at* [www.ftc.gov/os/caselist/0923093/100624twittercmpt.pdf](http://www.ftc.gov/os/caselist/0923093/100624twittercmpt.pdf).

83. *Id.* at 4.

84. *Id.* at 5.

85. *Id.* at 4.

86. *Id.* at 5.

87. *In re Twitter, Inc.*, Dkt. No. C-4316, 092-3093 (FTC 2011) (order and decision), *available at* [www.ftc.gov/os/caselist/0923093/110311twitterdo.pdf](http://www.ftc.gov/os/caselist/0923093/110311twitterdo.pdf).

88. *In re Google Buzz*, EPIC.ORG, <http://epic.org/privacy/ftc/googlebuzz/> (last visited Aug. 25, 2011).

89. Cecilia Kang, *Privacy Advocates File FTC Complaint on Google Buzz*, WASHINGTONPOST.COM BLOG (Feb. 17, 2010, 7 a.m.), [http://voices.washingtonpost.com/posttech/2010/02/privacy\\_advocates\\_file.html](http://voices.washingtonpost.com/posttech/2010/02/privacy_advocates_file.html).

90. Harriet J., *Fuck You, Google*, FUGITIVUS BLOG (Feb. 11, 2010), <http://fugitivus.wordpress.com/2010/02/11/fuck-you-google/> ("[I]t's SO EXCITING, Google,

that you AUTOMATICALLY allowed all my most frequent contacts access to my Reader.”) (emphasis in original).

91. *Id.*

92. Complaint of the Electronic Privacy Information Center to the FTC, *In re Google, Inc.*, at 4, available at [http://epic.org/privacy/ftc/googlebuzz/Google-Buzz\\_Complaint.pdf](http://epic.org/privacy/ftc/googlebuzz/Google-Buzz_Complaint.pdf).

93. Miguel Helft, *Anger Leads to Apology from Google About Buzz*, N.Y. TIMES (Feb. 14, 2010), [www.nytimes.com/2010/02/15/technology/internet/15google.html](http://www.nytimes.com/2010/02/15/technology/internet/15google.html).

94. Press Release, Fed. Trade Comm’n, FTC Charges Deceptive Privacy Practices in Google’s Rollout of Its Buzz Social Network (Mar. 30, 2011), available at [www.ftc.gov/opa/2011/03/google.shtm](http://www.ftc.gov/opa/2011/03/google.shtm).

95. *In re Google, Inc.*, No. 102-3136,

Decision and Order (Oct. 13, 2011), available at [www.ftc.gov/os/caselist/1023136/index.shtm](http://www.ftc.gov/os/caselist/1023136/index.shtm) (“[Google] shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to: (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information.”).

96. *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008); accord *United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010), cert. denied, 131 S. Ct. 1513 (2011).

97. See, e.g., Robert Sprague, *Rethinking Information Privacy in an Age of Online Transparency*, 25 HOFSTRA LAB. & EMP.

L.J. 395, 409–10 (Spring 2008) (recognizing “the possibility that a person could publish personal information to their blog or social networking profile, retaining its privacy even though the information may be available to anyone with an Internet connection. The intent in publishing the information is often only to share it with a few friends; the fact that it is widely accessible is an indirect consequence.”); Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 970 (2005) (arguing, based on studies of how information gets disseminated by various groups, that “certain groups can be designed to trigger reciprocal nondisclosure, and people making germane disclosures within these settings generally ought to expect that the information will not circulate outside the group”).