What Anyone Can Know

The Privacy Risks of Social Networking Sites

For the Net generation, social networking sites have become the preferred forum for social interactions, from posturing and role playing to simply sounding off. However, because such forums are relatively easy to access, posted content can be reviewed by anyone with an interest in the users' personal information.

David Rosenblum
Harvard University

In 1992, when I was five, my parents bought me my first computer—a Mac with 40 megabytes of memory that bore little resemblance to the digital technologies we take for granted today—but it was the beginning of a love affair. Like many others my age, I've grown up in a world of sensory overload, continuously connected to instant messaging, always reachable by cell phone. My generation lives in a world where communication is virtually instantaneous, and vast amounts of information are available at the touch of a key. In such a technologically saturated and digitally defined environment, we take it for granted that almost any information can be sourced on the Net. We post our opinions and live our daily lives online. But this complacence, when combined with chat rooms, message boards, blogs, and social networking sites such as MySpace (www.myspace.com) and Facebook (www.facebook.com), can prove embarrassing or even dangerous.

The potential exposure of posting personal information on such sites has received more media attention recently as the first suits arising from contacts originating in these sites have reached the courts.[1-3] These cases, which include alleged assault and damage to reputation, suggest some of the risks involved in casually treating social networks as personal diaries. And the scrutiny that these cases have generated has, in turn, prompted social networks to introduce some recent access restrictions and more stringent privacy policies to protect against the illegitimate or unauthorized use of posted information. But despite such an increase in security protection by both site providers and users, as the Net becomes the preferred social forum for young adults, our private lives will increasingly be lived out in the public domain with the loss of a reasonable expectation of privacy protection for our personal information.

This article examines some of the risks social network site users face (primarily to their future educational and career opportunities) in casually posting personal information on a digital medium that creates a permanent record not only of their indiscretions and failures of judgment, but also of third-party commentary that might reflect badly on the poster. Because there is currently no technical silver bullet to purge inappropriate or damaging information once it has been broadly disseminated on a social network site, the optimal strategy for damage control in the absence of more aggressive content or user restrictions (or of site surveillance by site hosts) is simply to exercise judgment in what personal information we choose to post. Although this will necessarily have some chilling effect on the fluid, no-holds-barred ethos of these sites, it is the only thing that offers the hope of safeguarding reputation and privacy.

The evolution of social networking sites

For the generation raised with blogging, webcams, and icons of smiley faces that act as digital proxies for personal interactions, the distinction between private conversation and public disclosure has become increasingly blurred. The first online social networks evolved largely around gamers who built personas, engaged in weekly play, joined guilds, and shared views on game forums. These individuals were often involved in massive multiplayer online role-playing games (MMORPGs)—like *World of Warcraft*—which grew out of video games and allowed many players to play online together on the same screen through online servers. These virtual worlds had their own bulletin boards and instant-messaging (IM) channels that were restricted exclusively to members. Gamers customarily played through avatars (created virtual identities). *Second Life* is a recent virtual online world in which its members design every aspect of the world—from architecture to the social structures to the characters through which members *live* online. It is a virtual parallel universe in which every member is given an avatar or 3D body of his or her own unique design. Members of *Second Life* have virtual jobs, families, and friends.

Such virtual environments provide relative anonymity. Bulletin boards (where the gamers might post controversial opinions) are limited to guild members, and the virtual worlds are viewed as parallel worlds. The political analogue of gaming culture is the free-wheeling blog culture, which provides a forum for a variety of political viewpoints, including non-mainstream views. Social network sites are the natural outgrowth of these sites and carry with them the frontier mentality of Net culture. Instead of meeting to role play or exchange ideas, however, people simply meet. Social networks evolved to give users virtual hangouts where they could be themselves, share what they were working on, or just express their views. As Michelle Andrews observed in her *U.S. News and World Report* article, "social network sites … may not seem to qualify as social gathering spots, [but] for teens, they function very much like the malls and burger joints of earlier eras. They're where young people go to hang out, gossip, posture, and generally figure out how the world works."[4] As the name MySpace suggests, this was a space that would be relatively free of any adult monitoring.

But what began for net-savvy teenagers as a logical social extension of their virtual-world role playing is now having profound real-world ramifications as digital social networks become a seamless extension of real-world activities. Digital personas are increasingly scrutinized by third parties who do not necessarily share the Net culture's free-wheeling values. Whereas the original gaming networks were relatively autonomous worlds peopled by techies and insiders, social networks routinely involve activities and relationships that spill over outside the Net and require disclosure of more private information. But because the fundamentally social function of these sites has not changed (users are still making friends, trading views, and baring their souls online), the presumption of relative anonymity has endured, even though it is increasingly unfounded.

What is more disturbing is that, increasingly, access to personal information by unrelated parties is not the product of the Net's porous nature or poor security in the design of such sites. Rather, it results from an assertion of a "right to know" by prospective employers, government agencies, or businesses collecting market data who want to retain the right to review our personal communications.

The sites: spaces, places, faces

The basic premise of MySpace, Facebook, and comparable social networking sites is that their users can create personal profile pages where they can share everything from pithy social commentaries to compromising photos of themselves doing a keg stand or riding a toy dino.[5]

MySpace

The largest and by far the most successful of these sites is MySpace, which currently has 100 million profiles, with 270,000 new members signing up every day. In August 2006, MySpace represented more than 80 percent of all visitors to social networking sites. According to a recent survey by HitWise, a group that monitors Web traffic, MySpace is the largest single source of Web traffic to Google.[6]

Users and friends. There are a variety of different users of MySpace, from fledgling musicians, artists, and photographers, who launch their work through the nearly endless array of forums and specialty sections, to homegrown Sylvia Plath wannabes who post teenage poetry and bombard the visitor with Morrisey songs. As the "Music on MySpace" sidebar suggests, musicians have colonized a sizable section of MySpace to promote their work and to stay connected with their fan bases. Because MySpace is a social space, it is peopled by predictable social cliques whose profiles show a remarkable self-selecting homogeneity. A quick keyword search for, say, *goth chicks who like Pink Floyd and eat their peanut butter sandwiches à la Elvis with bananas*, will turn up legions of like-minded individuals. This makes MySpace the most effective social search engine ever created, and—after barely two years—the fourth most popular site in the US behind Google, Yahoo, and MSN.

MySpace offers a forum where individuals can post thumbnail sketches of themselves, their antics, tastes in music, political views, and favorite quotes—in short, anything that might form the basis of a social connection to Net friends. *Friends*[7] is the term applied to members of a social network who list on someone else's page, and it includes both actual longtime friends and strangers who communicate online only.[4,7] In a world where friendships are mediated through a digital interface, *friendship* is defined as the regularity of the visits to one's page. Members of an online network can ask to be listed on a user's friends list and this will provide a link to their own profiles as well. Like any other social environment, browsers seek people who share similar interests, and a virtual circle of friends is created. Even if there is some question as to whether the term friendship can legitimately be applied to regular digital contact, there is little doubt that the function of such sites is social, allowing the members of a generation to ally themselves with others who share their worldviews. Social networks currently attract nearly half of all users of the Net (an estimate based on the number of visitors to the top 10 social network sites).[8] Such sites have recently evolved to provide integrated search engines as well.[9]

Advertising and self-promotion. What is particularly interesting about MySpace is the emphasis it places on self-promotion. In fact, personal profiles are often referred to as advertisements, and some profiles are just that—character profiles that are launched by businesses, or as movie promotions, to generate a fan base or create a buzz for an upcoming movie, new release, or new product. Users describe this as a sort of stealth marketing or merchandizing, because it is difficult to tell the difference between a genuine profile and constructed promotional one. Given that adolescent posturing often blurs the line between an offline personality and the fictionalized persona designed to explore a virtual-realm identity that is dangerous to explore offline, the distinction might revolve around what feels exploitative to users rather than what is real.

Stealth advertisers are exploiting the power of friendships as a sales or marketing tool. As one Fox News Corp. executive noted, "The real appeal to advertisers is the opportunity to create personal relationships with millions of actual young people. What we really struck upon is the power of friendship."[7] It's not clear that MySpace users want their friendships creating revenue for Fox. But it is a forum in which individuals advertise themselves as potential friends to a large peer audience and often pursue a kind of Darwinian social competition (or collector's mentality) in assembling as large a friends list as they can with almost no regard to who gains access to their intimate thoughts and information. As Andrews notes, "Some teens will accept total strangers as friends in an attempt to boost the total number of friends noted on their page, and so appear popular."[4] It is common for a simple request from a stranger to be listed as a friend to be sufficient to add that person to the friends list.

MySpace personal profiles are carefully produced personal brochures, and friend lists are a way of showcasing acceptance. One student candidly admitted, in an article for *The New York Times*, that she accepts any and all friend requests she receives. Another frequent user described her "strategy" for attracting new friends: "Pictures are extremely necessary for enticing new friends—the more pictures the better. … Every profile is a carefully planned media campaign."[10] Social networking sites are digital popularity contests with success measured in the number of unsolicited hits to one's page, as one user of multiple social network sites observed in the same article: "I click through the profiles of my friends to the profiles of their friends (and their friends of friends and so on), always aware of the little bar at the top of each profile page indicating my multiple connections. …I am obsessed with testimonials and solicit them incessantly, they are the ultimate social currency, the public declaration of the intimacy status of [our] relationship."[10]

These sites are the current currency of social validation and, to ensure that that currency is not counterfeit, the testimonials contained must be public. The legitimacy of the social environment demands that posts be uncensored. Indeed, the very rationale of these sites encourages exaggerated or outlandish self-expression "intended to show how funny, cool, or outrageous [the posters] are,"[11] according to another *New York Times* article. These sites are a bulwark of First Amendment expression. But they are also unwitting clearing houses for unauthorized personal information and, increasingly, these sites are converting social friendships into lucrative branding platforms: "YouTube's effort to make money out of its online audience … by encouraging users to create their own ads is a further sign that social networking sites are becoming powerful branding platforms."[12]

Limits and restrictions. In virtually all the social networking sites, from MySpace to Facebook to Friendster, there are few meaningful restrictions on access or the posting and transfer of information. *Wired News* recently reported that MySpace dedicates one third of its staff to "looking at images and profiles that potentially violate the site terms of use."[13] However, the site has only 300 employees. With "270,000 new users registering every day and also a thorny tangle of privacy and legal issues to navigate, MySpace doesn't aspire to keep tabs on everybody."[13] According to MySpace, its staff members, "eyeball each of the 3 million images that are posted each day, searching for—and removing—nudity, hate speech or symbols, and offensive content." However photos that are merely provocative are not removed.[13]

Personal profiles are readily available to anyone who registers and there are few (if any) limitations on who might register. As the sidebar, "The Porous World of MySpace," describes, I did so in less than five minutes, providing largely fabricated and somewhat inflammatory personal information. *Wired News* noted that "Users can easily register and start using MySpace with a completely fake name, address, age, and even email address, and one suspects that many people who wish to use the site for ill purposes often do just that."[13] There is little incentive for the site to change this, however, because requiring personal verification could potentially destroy the "open" culture that is the foundation of the site's popularity, and drive off its user base. "It's a loophole that the site has no intention of closing."[13] Moreover, through links to friends, blogs, and related sites, postings can be broadcast throughout the Web almost instantaneously.

Facebook

If MySpace highlights its pages' creators, and is as much a form of entertainment dedicated to promoting the art

Music on MySpace

New musical artists—as well as many established ones like Dashboard Confessional, Fall Out Boy, and Head Automatica—use MySpace as an informal bandlog or bulletin board to publicize performances and new releases because their target audience is already assembled online. They create band profiles, post music downloads, and provide live video streaming for their fan bases. In the music industry, it is currently considered essential for breaking artists to have cutting-edge pages on MySpace. And MySpace now offers music downloads for purchase as well.

In September 2006, MySpace launched its online music store to compete with Apple's iTunes Music Store.[1] MySpace will offer music for sale through a partnership with Snocap (the tech company developed by Shawn Fanning, creator of the now legendary Napster). Bands or labels of any size can sell songs at a price they set, but MySpace will take a fixed fee. Songs are available for purchase in MP3 format, which is compatible with Apple iPod but doesn't provide copy protection. It is unlikely that major labels will sell in this format because of the lack of protection against ripping (copying multiple copies). Once it is downloaded, MP3 format can be freely copied and shared without technical restrictions. In my own experience as a musician, I have avoided MySpace, preferring instead to launch myself via the more underground Sonicjive.com.

Reference

1. R. Levine, "MySpace Music Store is New Challenge for Big Labels," *The New York Times*, 4 Sept. 2006; www.nytimes.com/2006/09/04/technology/04myspace.html.

products of its posters, Facebook is much truer to the model of social networking. A later arrival than MySpace, Facebook is rapidly becoming as popular, if not more so, and was listed among the top 10 Web sites in 2006.[8] Although the site has a more limited range of functions (no blasting punk-pop music or live video feeds), it is arguably more effective as a tool for social interactions. Instead of throwing the user into a cumbersome, and at times bewildering, matrix of people and connections, it bases its network on an already well-established one: college affiliation.

User profiles. Although the site's restricted focus would seem to simplify the security challenges—access to the site can be limited to the targeted community—Facebook presents its own unique set of risks. Far more information is provided on the typical Facebook profile than on a comparable MySpace profile. And, while access is limited to registered users on the poster's college network or friends that have specifically been allowed to see a profile, the fact that users frequently list full names, home addresses, AOL Instant Messenger (AIM) screen names, email addresses, and sometimes cell phone numbers, makes such limits illusory.

Limits and restrictions. Options have been added recently to prevent uninvited contact with underage users,[13] but few have taken advantage of these protections. As Michael Calore noted in a *Wired News* article, "Facebook users filling out a profile have all consciously chosen a certain level of transparency. Online communities encourage open sharing, so, even though privacy controls are in place for most of these tools, many users publish publicly anyway."[14]

Although Facebook requires a college email address for registration, many network users maintain their accounts long after they have graduated. The only real effect of this minimal restriction is to encourage an unwarranted presumption of privacy, because there is no effective way to police who is actually using a valid account. And, although ethical questions are raised when an unauthorized user (one whose interest is not primarily social) reviews personal data, there is no way to secure these sites against it. Youthful "indiscretions" or posturing, and the exaggerated role playing that social networks encourage, can become career liabilities, because the limited audience to which the post was directed is not the only audience actively viewing it.

Presumptions of privacy in a virtual space

It is possible to glean personal information even without accessing a home page on these sites because many people use the public wall as a private message board to post intimate details of their lives, schedules, or recent sexual conquests. But what would motivate people to broadcast their private lives? As one user explained it: "Like many of my generation, I consistently trade actual human contact for the more reliable high of smiles on MySpace, winks on Match.com, and pokes on Facebook. I live for Friendster views, profile comments, and the Dodgeball messages that clog my cell phone every night."[10]

Online intimacy

The key concept for understanding what fuels these sites is intimacy. Social communication is intrinsically personal and, even if it occurs in a digitally mediated context, it fulfills the fundamental need for connectedness—the feeling of belonging. To understand the notion of Net intimacy, it is important to look at a network like Dodgeball, which one user described this way: "It is the most intimate and invasive network I belong to. It links my online communications to my cell phone, so when I send a text message to

36343_[Dodge], the program pings out a message with my location to all the people in my network. … Acceptance into another person's Dodgeball network is a very personal way to say you want to hang out."[10] The words themselves (intimate and invasive) indicate how irreconcilable such networks are with traditional ideas of privacy. A Google map allows any member to retrace the steps of any other member, "tracking their paths through various bars."[10]

The porous nature of the Net has radically redefined the arena in which individuals are willing to disclose personal information.

This is intimacy at a digital remove—virtual voyeurism for a generation with fears of commitment, as the same user observed: "I prefer…a world cloaked in virtual intimacy. It may be electronic, but it is intimacy nevertheless. Online, everyone has bulletproof social armor." She further described her motives: "I am constantly searching the Internet for new communities. I need to belong to all of them because each one enables me to connect to people with different level of social intimacy." She is thus spared "awkward social situations I couldn't log out of."[10] Online intimacy is not a substitute for intimacy, however. It is the authentic social experience, as the young woman observed of neighborhood friends: "We have enough connection online for our degree of closeness, and don't need to enhance our relationships by spending time together offline."[10] It's difficult not to wonder if virtual intimacy allows a generation to avoid intimacy altogether by protecting them from the real-world interpersonal growth that comes with not being able to log off.

Privacy redefined

Last August, Facebook added a feature called "News Feed," which automatically alerted everyone on a user's friends list to any changes to the user's page and to any new posts. Personal information that users "posted selectively in a matter of hours became uncomfortably public."[15] For example, when someone I barely knew was told by his girlfriend that their relationship had crashed and burned, I knew it at virtually the same moment he did. It is understandable that users would want sensitive personal information to be communicated only to those close friends who visit their pages regularly. The outcry that resulted from the introduction of News Feed clearly indicated that "the exhibitionism and voyeurism implied by participation in social network sites has ill-defined but nonetheless very real limits, and the expectations of privacy have somehow survived the publishing free-for-all."[14] Users clearly still believe that their communications are "private" in some sense. And yet, traditional notions of privacy are fundamentally antithetical to the rationale of the Net.

When Tim Berners-Lee first envisioned the World Wide Web, he imagined a global network for "decentralized, organic growth of ideas, technology, and society."[5] People from all around the world would be able to express their thoughts in the intimacy of a virtual environment. Berners-Lee understood what the First Amendment embodies—the belief that the democratization of information leads to greater freedom and to the unfettered development of ideas. Anglo-American contract law is founded on the notion that the free flow of information will ultimately promote more equitable contracting, and free market economic theory is premised on equal and unrestricted access to information. Our modern democratic institutions presume that any interference with the free flow of information will lead to social injustice. The Web is a virtual soapbox. Any constraint on its content is presumed by the evolving case law to have a chilling effect on free speech,[16] hampering the productive growth of ideas and of society. Although the free speech concerns raised by the Net are beyond the this article's scope, it is important to understand the breadth of the protections currently afforded to Net speech in order to grasp the openness of Net culture and the expansive scope of the free expression that individuals feel entitled to exercise online.

Blurring the public/private line

The porous nature of the Net has radically redefined the arena in which individuals are willing to disclose personal information. The comfort zone of the Net generation is much larger and its circle of friends more broadly defined. The distinction between public and private is further blurred by a generation Michael Block has characterized as "starved for attention."[5] The Net generation has been raised on the voyeuristic model of reality TV, and on the notion that it is appropriate to showcase one's questionable judgments in front of a wide public audience: "Our everyday culture definitely celebrates self-disclosure. [It] has sent the message that acting stupid in front of a camera is a way to get attention or to start a career,"[5] as Block notes. For many, it is also a way of defining oneself.

One social network user recently wrote: "every morning before I brush my teeth I sign into my Instant Messenger to let everyone know that I'm awake. I check for new emails, messages, views, bulletins, invitations, friends requests, and comments on my blog, or mentions of me or my blog on my friends' blogs."[10] As the title of *MySpace Nation*[5] implies, this is a generation whose identity has been forged online; having a page at one or more of these sites is the modern rite of passage. And just as sound bites shape the news for an increasingly time-constrained culture, so "tagging" (the digital equivalent of a highlighter pen for personality traits) shapes and defines a user's online identity or circle of friends. Tagging is the activity of using keywords to help others with similar interests link to the content of a user's profile. If I'm an anime fan, I might highlight anime, or Japanese pop culture, or "J Pop." Essentially, it's a shorthand way to forge an online social group from keyword compatibility.

The hybrid nature of Net culture

Part of the explanation for the willingness of individuals to post private information on the Net is Net culture itself. The Net generation is engaged in free exercise in the truest sense. What creates the security risk is the presumption of privacy that accompanies this exercise. Like the virtual denizens who inhabit *Second Life*, the members of social networks believe that their networks are private virtual worlds where Net rules and Net ethics apply. Although these networks might parallel the offline world, they have retained some of the fantasy and role-playing aspects of virtual worlds. It is difficult for their users to grasp that actions and speech within the online networks can have profound ramifications offline. "Regular MySpace users, however, can get caught up in sharing their daily dramas and escapades—so engrossed that they sometimes forget the whole world may be watching. There have been…news reports of police nabbing teens who bragged about or posted pictures of their illegal exploits," Andrews writes, but "more commonplace … are photos and postings detailing underage drinking and pot smoking that could conceivably hurt teens' chances when they apply to college or look for a job.…about a third of employers screen job candidates using search engines like Google, while 11.5 percent said that they look at social network sites."[4]

Security and privacy risks

Just as jurisdictional case law has had great difficulty defining the nature of the virtual world's space,[17,18] so privacy law has not developed a language for determining when the digital speaker has a legitimate expectation of privacy. Digital publication of images has been analogized to broadcast media.[19,20] How then do we conceptualize digital utterances (or posts) within social networks? MySpace, Facebook, and similar sites have clearly been designed around Berners-Lee's original premise that people from all around the world should meet and share ideas in a relatively uncensored environment. Like everything else about the virtual landscape, however, the potentially limitless dissemination of information almost instantaneously alters the fundamental nature of the speech.

Internal risks: Net speech and broad dissemination

If I am out with friends at a bar and express a controversial view, the context assures me relative anonymity. I can look around and determine if my comments will go farther than those four walls. The social environment condones and shelters a free-wheeling banter. There is no permanent record of my views for attribution except word of mouth repetition for which there is plausible deniability: "I would never say something that stupid." Finally, no one is systematically screening my remarks to "harvest" social information, or attempting to "monetize" my friendship circle.

The assumptions that justify (and make "reasonable") a presumption of privacy with respect to intimate social communications are unfounded in the context of the Net. From the vantage point of my bedroom computer, I lack even the minimal social cues of a Friday night bar that I am in a quasi-public situation. Indeed, all the physical evidence tells me that I can drop my guard. Unless I am on webcam, I can sit in my underwear, scratch my stomach, and belch. The only tangible audience for my utterance is the monitor. However, if we were to draw a real-world analogy to posting on MySpace, it would be more analogous to taking a megaphone into Madison Square Garden each time I typed in a message (there's a reason they are called "posts"). That is not the mental image we have of our virtual chatting, and this is what creates the security exposure—not simply the relatively porous nature of social network sites, but the lack of any realistic sense of how public or how permanent the record of our utterances is. This artificial sense of the anonymity of Net communications leads people to actually lower their inhibitions, and to feel protected from the consequences of their speech.

Users are communicating in their virtual underwear with few inhibitions. In addition, they are posturing, role playing, being ironic, test-driving their new-found cynicism in instantaneously transmitted typed communications or instant messages. And all this on a medium that does not record irony (unless you cue in the little smiley face icons). The valence of language that allows tone to control meaning is lost. There's no hot button for *are you kidding*? But as the media has learned with sound bites, limiting the context of an utterance can radically distort its meaning. Nothing could manipulate a context more than stripping our utterances of their nuances. This is a new language universe, one in which context must be interpolated with little evidence beyond printed words. The new mall is word-based.[4] What these social networks encourage is a culture of ambiguous signifiers which the reader is left to interpret. If a reader happens to be a hiring officer, this can have disastrous results. In addition, where my bar indiscretions might get some replay the next day, the listeners' own fears of having made similar gaffs will act as a kind of check on the broad dissemination of my remarks. Not so on the Net, where communication is recorded in permanent form. It is broadly disseminated, multiply stored in countless independent permanent storages, and can be retransmitted with the click of a button. Next-day damage control is almost impossible. I cannot say: "Oh no, that's not what I said." The record's permanence makes any such protest moot.

And finally, there is a search engine: anyone who has missed what I said, or who might have more than a passing interest in my lapses of judgment, can find my remark quickly and efficiently with a few clicks. I've made a fool of myself on a scale much larger than Madison Square Garden and a megaphone.

External security risks: Unauthorized use by third parties

Although MySpace was originally conceived as a safe, self-defining social network, it has become a kind of nonconsensual reality blog. In the process, the nature of the presumed audience has changed, and with it any presumption of privacy. That the original "audience" with access to MySpace posts was large does not automatically negate a presumption of privacy or of reasonable limits on how its posts could subsequently be used. But because MySpace is increasingly being used as a public database for personal information, evolving custom has had a profound impact on the nature of the forum and the notion of fair use of posted speech. At some point, a porous medium, public scrutiny and knowledge of the potential risk will make a forum public. The enormous potential market, coupled with the information opportunity presented by such a database, will make such a transformation almost inevitable.

Security risks are created not merely by the injudicious remarks of a generation using social networks as a combination of chat room and second life, but also, and more importantly, by the co-opting of a large, autonomous, and initially private network for corporate gain—whether intelligence gathering or profit making. As the technology journalist John Batelle recently noted, "We assumed the digital footprints we left behind—our clickstream exhaust, so to speak—were as ephemeral as a phone call, fleeting, passing, unrecorded. …Our tracks through the digital sand are [in fact] eternal."[21] We are building monuments, and not particularly flattering ones.[22]

Prospective employers. The most immediate danger of posting is the obvious one of leaving a permanent digital record of compromising pictures and remarks that can later be searched and accessed by third parties trying to evaluate the character of an applicant for a job, school admission, or other competitive position for which applicants must be screened and eliminated. The Net is a virtual landscape of *ex parte* communications that could prove damaging to careers and academic opportunities, if viewed outside their original social context. Because so many profiles contain third-party comments or communications, the temptation to condemn an individual for uncensored or injudicious posts to friends is great.

A recent *New York Times* article describes how one hiring officer lost interest in a promising applicant when he discovered through Web chat that the applicant was interested in "smoking blunts, shooting people, and obsessive sex."[11] Although the officer understood that the remarks were largely the product of Net posturing, and should not be taken at face value, their publication on the Net caused him to question the applicant's judgment. As the company president succinctly put it: "Why are you allowing this to be viewed publicly, effectively?"[11]

Companies now routinely use search engines to do their background checks on prospective employees, and also often review social networking sites (specifically MySpace) where students post "provocative comments about drinking, recreational drug use, and sexual exploits in what some mistakenly believe is relative privacy."[11] While many officers acknowledge that they are reviewing information they would not otherwise have the legitimate right to solicit, they justify this practice by the public nature of these sites. As one officer observed: "You really do get a lot of information you can't ask for in the job interview, but you go on the Web and it's all right there."[23] Companies use the information as a kind of vocational Rorschach to determine whether there is "something about their lifestyles that we might find questionable, or that we might find would go against the core values of our corporation."[11] Such an inquiry clearly implicates First Amendment concerns.

Corporate opportunists. To make matters even worse, there are large marketing conglomerates, like News Corp., the parent company of Fox network, buying up sites like MySpace to capitalize on the market opportunity presented by social networking.[24] Two immediate concerns arise from this. First, Fox is known for its voyeuristic, sensational approach to news and media. MySpace already suffers from the innocent-adolescent-brand voyeurism that comes with teens posturing for a peer audience; the site has recently been battered by assault charges stemming from sexual predators contacting underage members (in a much more dangerous, and more socially exploitative form of voyeurism).[13] Now, MySpace might be forced to add to this the Fox treatment of reality-TV voyeurism. Second, there is recent precedent for a carrier asserting exclusive ownership of the digital content of its email traffic. In June 2006, AT&T instituted a new privacy policy stating that the company, not customers, owned the customers' private data.[25] Fox could claim ownership of and exploit the content of MySpace, either using personal information in any way it saw fit or selling the right to use it to others.

Large news conglomerates are just beginning to appreciate the value of social networks as an advertising medium, a captive audience, a commodity-indicator of purchasing preferences, and a kind of shorthand record of demographic trends. An entire generation's tastes can be

The porous world of MySpace

MySpace recently offered members an option to limit access to their personal information. To test the effectiveness of the registration limitations and the amount of personal information that could be gleaned from a quick search—that is, to test the degree to which posters are heeding the new MySpace options and safety tips—I signed on under the fabricated identity of a 34-year-old male. Registration took under five minutes, even though my profile was expressly designed to raise concerns, in light of my description of my interests and my age. MySpace expressly states that it will delete any profile that lies about age.

Once signed on, I clicked on and reviewed the first profile I scrolled to. The woman I chose at random was generally careful about the information she posted. To her credit, she included her age, but not her birth date; home state, but not the town; first name, but not last. However, these cautions were mooted by the fact that she posted pictures of herself. Although pictures are difficult to search without an electronic signature, other posted information could be used to narrow a search. Most important, she posted her AOL Instant Messenger screen name. This linked her home page to her blog, which provided enough information to determine her name.

Cursory examination of her blog brought me to a 6/6/06 post that described her visit to Hell Michigan, and was less than reassuring to a potential employer. Two noteworthy pictures included a sign advertising a "Devil's Day Hellfest," and a cartoon of Jesus being flogged entitled "Lord, Liar or Lunatic?" An only slightly less casual review of her blog posts revealed one titled "surveys," in which she posted her detailed responses to a number of online surveys. Among these were answers indicating that she had been medicated for attention-deficit disorder and obsessive-compulsive disorder behavior, and had been taken into police custody. She also candidly admitted to having stolen in the past. It is important to understand that all this information was readily available. A 10-minute search yielded enough damaging material to cause a hiring officer to reconsider an offer. And, far from being egregious, this profile was fairly conservative in the kind of personal information it contained.

micromonitored, micromanaged and manipulated: "Our very activity online has become a valuable commodity—an indicator of interest and therefore something to be measured, tracked, bought and sold, and archived by search magnates and data compilers."[21] MySpace has recently created a "clean" space where advertisers (like Disney) who don't want their products associated with the freewheeling blog culture or the accusations of soft porn and child exploitation can reach their target audience without being "associated with unsavory material."[26] News Corp. would like to turn MySpace into a full-service portal, competing as an independent search engine with Yahoo and Google. A significant part of the draw of this is clearly the social network's database. Not only are the private expressions of a generation being perused by stalkers, voyeurs, hiring officers, and government agencies, but they are being analyzed and marketed.

Social predators. Social network sites have already been exploited by sexual predators, stalkers, child molesters, and pornographers to approach minors.[1] In one recent incident, a 14-year-old girl filed a damage action for US$30 million against MySpace, alleging that she was sexually assaulted as a result of her contacts with a 19-year-old man on the site. Such suits demonstrate how online activities can have unforeseen and dangerous offline consequences. But they also suggest that users do not exercise in the virtual world even the routine common sense they would exercise in the real world. As one writer noted: "If kids follow their instincts and the same common sense they'd use walking to school, or going to the mall, it [MySpace] is remarkably safe."[27] The point is that most users don't exercise the same common sense, because they conceive of themselves as interacting in a protected environment. As a result of a mistaken perception of relative safety, "the information that kids share today is personal and private information that allows predators to track them down."[2] Social sites also create the potential for "cyberbullying" by peers. Users often receive unsolicited messages that are obscene, inappropriate, or even threatening. In one case, a 15-year-old girl was subjected to repeated death threats on MySpace from two older teenage girls, who threatened to smash the girl's head in and slit her throat.[3] Other users have been criminally charged for threatening posts, including two eighth graders who posted a Columbine scenario.

Site operator responses

All these threats have caused social networking sites to increase access restrictions. Networks have responded with a variety of new measures, including greater privacy settings that allow their members to limit access to their pages to people they know or people who have a verifiable network registration. MySpace recently proposed options to make it more difficult for strangers and users over 18 to contact users under 16, and also allows its members to designate their profiles as private, which will limit access only to designated "friends." Although MySpace encourages users under 16 to make their profiles private, profiles of users over 18 are routinely accessible by any visitor to the site, and MySpace does nothing to verify its users' ages. News Corp. explains their new safety options as a way to offer protection while not "clamping down on the freewheeling and flirtatious interchanges that are the source of [the site's] appeal.

…We want to balance the openness of our community with the interest of protecting the members."[1]

Several Net groups have recently built a central database to identify pornographic images of children sent by email.[2] This effort comes largely as a response to recent US Attorney General requests for Internet companies to preserve email data for evidence of unlawful activity. The US Justice Department would like networks and carriers to retain records of their users' Web correspondence for two years. Internet companies have resisted the retention and policing of user email, because it "might compromise the privacy of their users."[2] Currently, AOL scans all email traffic for electronic signature matches with pornographic images it has been made aware of. But more disturbing, from the point of view of users' privacy, is the recently publicized disclosure of "secret rooms" at AT&T buildings, where government personnel are reported to have "gained access to millions of private email messages and other Internet traffic."[28] According to a recent *New York Times* article, the US National Security Agency is "financing research into the mass harvesting of information that people post about themselves on social networks like MySpace."[25] "Data" collected in this manner "could be combined with details such as banking, retail, and property records, allowing the NSA to build extensive all-embracing personal profiles of individuals."[25] Such intrusive surveillance does not balance the concern for security with the right to privacy.

It is hardly surprising, however, that the Net offers a ready database for personal information that can be efficiently and anonymously harvested, via search engines, by unintended users. It goes without saying that a marketplace for personality profiles will necessarily draw other users of such data, like the hiring officers discussed earlier, government agencies, and advertising or market research professionals trying to identify and exploit buying trends. Networks also provide an opportunity for law enforcement agencies to search criminal behavior through personality profiles. In one horrific recent case, a multiple murderer was exposed through Net statements about his murderous fantasies. Moreover, in the post-9/11 security climate, the temptation is great to review political speech for controversial and unpopular views, and to create government records of individuals holding those views. Such surveillance poses a serious threat to open political debate. I'd hope we learned from McCarthyism the dangers of witch-hunting political subversives. But, as Batelle notes, "The digital trail—the wide wake we tend to leave as we transact an electronically mediated life"[21] can have repercussions in unrelated areas. "It's easy to forget the power of the technology now at our fingertips and the persistence of the data that it allows us to manipulate—in all its forms. We underestimate its reach, its potential to backfire in shifting contexts, and the loss of control we suffer when our words and images are set adrift."[21]

Common sense solutions

There is little that can be done from a technical point of view to change the intrinsically porous nature of a digital medium; there is also little or no incentive to create personal information verification procedures or enhanced scrutiny with regard to posted information, because both could potentially chill the almost-anything-goes ethos of the social networking sites. This ethos is the foundation of the social network site base, and of a hugely lucrative potential marketing network. Such a chilling effect on the content of these sites would also raise important First Amendment issues.

From an economic and legal point of view, therefore, it is unlikely (in the absence of onerous damage actions against such sites) that site operators will take any meaningful action to decrease the potentially damaging exposure of posters' personal information. The users themselves must then exercise some self-limiting common sense either in reviewing what they post, or in periodically reviewing what is available online about themselves. In this manner, they can take some control of the digital profile that third parties see. They might also try to encourage these sites to provide mechanisms whereby they can purge any unwarranted, damaging or inflammatory information from these sites. MySpace claims that such a service is readily available. The latter, however, is only a partial solution. MySpace is not a closed universe. Once any information is widely disseminated, it is all but impossible to purge every iteration outside the social network.

The most frequently identified risk of morphing our social lives and personal communications into the digital era (in addition to the broad and indiscriminate dissemination of our every thought and compromising photo) is that there is no longer an expectation of privacy in the sphere that traditionally has been the core of our self-conceived private lives. If prospective employers or university admission officers want in-depth access to a candidate's personal activity, they can access these sites (either directly or through college-age staff members), and readily get an uncensored, unflattering, and in many cases largely unrepresentative portrait of that candidate. Not only is this information unfiltered by the selective editing of context (it was not prepared to show a candidate in the best light for a job interview, but rather to impress beer-swilling friends), but it is often deliberately skewed toward the exhibitionist, provocative, and inflammatory, as schoolyard showboating should be. Bonding is not the same social process as applying for a responsible job. We don't routinely bash chests with future employers. But if the very nature of the forum undermines our claim to privacy protection, the answer might be in *PC Magazine's* advice to users of MySpace that "[c]ertain information is best withheld from the public."[5] If not, an entire MySpace generation could realize, when it is much too late to intervene, that the cyber personae they spawned in adolescent efforts to explore identity have taken on permanent lives in the multiple archives of the digital world. □

References

1. S. Hansell, "MySpace to Add Restrictions to Protect Younger Teenagers," *The New York Times*, 21 June 2006; www.nytimes.com/2006/06/21/technology/21myspace.html.
2. S. Hansell, "Online Effort is Planned against Child Pornography," *The New York Times*, 27 June 2006; www.nytimes.com/2006/06/27/technology/27porn.html.
3. E. Ray, "2 Girls Sentenced for Threats on MySpace," *The Toledo Blade*, 28 June 2006; www.toledoblade.com/apps/pbcs.dll/article?AID=/20060628/NEWS02/60628049&SearchID=73278882340193.
4. M. Andrews, "Decoding MySpace," *U.S. News & World Report*, 18 Sept. 2006; www.usnews.com/usnews/news/articles/060910/18myspace.htm.
5. C. Metz, "MySpace Nation," *PC Magazine*, 21 June 2006; www.pcmag.com/article2/0,1759,1979264,00.asp.
6. D. Mitchell, "What's Online; MySpace No Longer Their Space," *The New York Times*, 3 June 2006; www.nytimes.com/2006/06/03/business/03online.html.
7. E. Holmes, "On MySpace Millions of Users Make 'Friends' With Ads," *The Wall Street J.*, 7 Aug. 2006, section B, p. 1.
8. A. Gonsalves, "Social Networks Attract Nearly Half Of All Web Users," TechWeb.com, 15 May 2006; www.techweb.com/wire/ebiz/187202833.
9. S. Olsen and E. Mills, "Google Pledges $900 Million for MySpace Honors," CNET News, 7 Aug. 2006; http://news.com.com/Google+pledges+900+million+for+MySpace+honors/2100-1032_3-6102952.html.
10. T. Stites, "Someone to Watch over Me (on a Google Map)," *The New York Times*, 9 July 2006; www.nytimes.com/2006/07/09/fashion/sundaystyles/09love.html.
11. A. Finder, "For Some, Online Persona Undermines a Resume," *The New York Times*, 11 June 2006; www.nytimes.com/2006/06/11/us/11recruit.html.
12. K. Allison, "YouTube Pushes Paris as the Way to Go," *Financial Times,* 22 Aug. 2006; http://search.ft.com/ftArticle?queryText=paris+hilton+you-tube&aje=true&id=060822009216.
13. J. Shreve, "MySpace Faces a Perp Problem," *Wired News*, 18 April 2006; www.wired.com/culture/lifestyle/news/2006/04/70675.
14. M. Calore, "Privacy Fears Shock Facebook," *Wired News*, 6 Sept. 2006; www.wired.com/science/discoveries/news/2006/09/71739.
15. J. Warrin and V. Vara, "New Facebook Features Have Members in Uproar," *The Wall Street J. Online*, 7 Sept. 2006; http://online.wsj.com/public/article/SB115759058710755893-iBS_PNU8HJZQfY8LaEBhLKh4aGc_20061006.html?mod=tff_main_tff_top.
16. "CDT Urges Court to Block French Net Content Restrictions in U.S.," *CDT Policy Post*, vol. 8, no. 10, 10 May 2002; www.cdt.org/publications/pp_8.10.shtml#1.
17. *Nissan Motor Co., Ltd., v. Nissan Computer Corp.*, *Federal Supplement, 2nd Series*, vol. 89, 2000, p. 1154 (US District Court for the Central District of California).
18. J. Zittrain, *Be Careful What You Ask For: Reconciling a Global Internet and Local Law*, research pub. no. 2003-03, Berkman Center for Internet and Society, May 2003; http://cyber.law.harvard.edu/home/2003-03.
19. *Yahoo v. La Ligue Contre Le racisme et L'Antisemitisme*, *Federal Supplement, 2nd Series*, vol. 145, 2001, p. 1168 (US District Court of Northern California).
20. *Zippo Manufacturing Co. v. Zippo Dot Com Inc.*, *Federal Supplement,* vol. 952, 1997, p. 1119 (US District Court for the Western District of Pennsylvania).
21. T. Zeller, Jr., "Link by Link; Lest We Regret Our Digital Breadcrumbs," *The New York Times*, 12 June 2006; www.nytimes.com/2006/06/12/technology/12link.html.
22. K. Allison, "Kinky Online Prank Rouses Fears over Privacy," *Financial Times*, 12 Sept. 2006; http://search.ft.com/ftArticle?queryText=kinky+online+prank&aje=true&id=060912007080.
23. P. Belluck, "Young People's Web Postings Worry Summer Camp Directors," *The New York Times*, 22 June 2006; www.nytimes.com/2006/06/22/technology/22camp.html.
24. R. Rosmarin, "The MySpace Economy," Forbes.com April 10, 2006; www.forbes.com/home/digitalentertainment/2006/04/07/myspace-google-murdoch-cx_rr_0410myspace.html.
25. D. Mitchell, "What's Online: More Rumblings About Net Privacy," *The New York Times*, 24 June 2006; www.nytimes.com/2006/06/24/business/24online.html.
26. J. Angwin, "MySpace Draws Ads by Offering 'Safe' Content," *The Wall Street J.*, 21 June 2006; http://online.wsj.com/public/article/SB115084367016885640-DsCpiNA71ulEatV9uPlRC1ig920_20060720.html?mod=tff_main_tff_top.
27. T. Zeller, Jr., "Link by Link; A Lesson for Parents on 'MySpace,'" *The New York Times*, 26 June 2006; www.nytimes.com/2006/06/26/technology/26link.html.
28. D. Mitchell, "What's Online; Publicly Debating Privacy," *The New York Times*, 27 May 2006; www.nytimes.com/2006/05/27/technology/27online.html.

***David Rosenblum** is a sophomore at Harvard University, majoring in government and minoring in East Asian Studies. His research interests include Internet security, Japanese "pop" culture, and copyright issues related to online music posting. He has written on jurisdiction and the Internet for a seminar at the Berkman Center for Internet and Society, and participated on an NYC Bar Association panel on Internet security and copyright issues. Contact him at darosenb@fas.harvard.edu.*