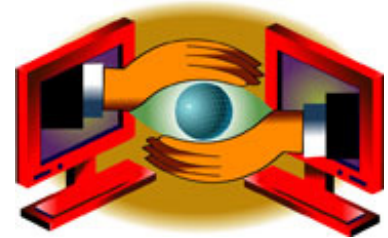




Unwitting Exposure: Does Posting Personal Information Online Mean Giving Up Privacy?

Published : October 04, 2006 in [Knowledge@Wharton](#)

The million-and-one ways in which the Internet can be useful, efficient and fun are well known. Its potential for abuse by pornographers, phishers, scammers and spammers has also been apparent since its early days. What has taken a bit more time to emerge, however, is awareness of the Internet's increasing threat to privacy as people become more comfortable offering information about themselves online.



This is a single/personal use copy of Knowledge@Wharton. For multiple copies, custom reprints, e-prints, posters or plaques, please contact PARS International: reprints@parsintl.com
P. (212) 221-9595 x407.

Faculty members at Wharton say people who access the Internet for what have become routine functions -- sending email, writing blogs, and posting photos and information about themselves on social networking sites -- do not realize how much of their personal privacy, their very identities, they put at risk. Nor do they fully comprehend the extent to which they are inviting mischief, embarrassment and harm, perhaps for decades to come, from others looking to dig up digital dirt. In addition, legal experts say that while laws already on the books provide criminal and civil remedies for some nefarious uses of personal information, the ways in which the Internet can be harnessed for questionable purposes that encroach on privacy have yet to be fully addressed by the courts.

Consider a few examples of how personal information and actions can take on a life of their own once they are posted on the Internet for all to see. In early September, a web developer took an apparently real advertisement placed online by a woman looking for a sexual liaison and posted it on the Seattle "casual encounters" section of the Craigslist bulletin board, according to press reports. There were 178 responses to the phony sexual solicitation, many of which included compromising photos. The developer then posted all the responses on a public website, including photos, email addresses and other personal information -- where anyone could view them.

Also in September, the social-networking site Facebook, which is popular among college and high school students, was the subject of protests by a number of users when it made some design changes. According to Reuters, more than 500,000 users complained about a new service called "News Feed" that instantly notifies members whenever friends post new photos or update information about themselves, such as their political affiliations and dating status. Users were angered, not necessarily because News Feed revealed personal data -- after all, the same information could be viewed in the user's profile -- but because it made it easier for users to track one another, said Reuters. "Stalking is supposed to be hard," one user said, according to the Reuters account.

The Federal Trade Commission announced on September 7 that Xanga, a social networking site popular among young people, will pay a \$1 million civil penalty to settle charges it violated the Children's Online Privacy Protection Act, which is the only federal statute on the books governing Internet privacy issues, according to legal scholars. Xanga collected, used and disclosed personal information from children under age 13 without first notifying parents and obtaining their consent, according to the FTC. The government said the penalty was the largest ever assessed for a violation of the child-privacy law.

Then there was the case of a young woman in Seoul who was on a subway train with her pet dog when the animal relieved itself on the floor. The woman did not clean up the mess, angering other riders, and the woman herself reportedly became surly as tensions escalated. Using a camera phone -- at 99%, South Korea has the highest camera-phone penetration in the world -- a passenger snapped a picture of the woman and the mess her dog had created. The photo, along with language describing what had happened, was posted online and eventually appeared on many sites. Some viewers were able to identify the woman,

who became such a pariah that she dropped out of college and went into hiding.

Other examples abound of how online information can be used, often quite legally, in ways that people never intended. How many job applicants have not been hired because prospective employers saw embarrassing online photos of them at parties? How many employees have been mortified when their critical email comments about their bosses or peers were circulated without their consent?

Who Owns You?

Anita L. Allen, professor of law and philosophy at the University of Pennsylvania and a leading expert on privacy issues, says the core questions raised by misuse of the Internet are not new.

"It goes way back to the general problem that people will use personal information that they can collect through surreptitious or open means to advance their interest at our expense," she says. "Gossip, which has been with us forever, is the same type of problem. As long as there have been businesses, there have been issues of confidentiality. There's nothing new there. What's new is the ease with which information can be collected and shared, and the ease with which it can be maintained for indefinite periods of time."

"In general, there has never been so much personal information about individuals as readily accessible as there is today with the Internet," adds [Kevin Werbach](#), professor of legal studies and business ethics at Wharton. "It's particularly so with social-networking sites. It's also the case that the younger generation -- teens and 20-somethings -- are by and large more comfortable with putting personal details on websites than prior generations."

Indeed, Werbach says he often discusses Internet privacy issues with his undergraduate students each semester. Whenever he asks how many of them post personal information on sites like MySpace and Facebook, just about every hand goes up.

"That being said, there's a difference between putting information on a purely public site, like your own website that's accessible to anyone in the world, and putting something on a site like Facebook, which is a controlled, private site available only to its members," Werbach notes. "The question of who owns the information on these sites is a very interesting one. Most have policies saying they have ownership of anything posted there, but clearly that doesn't give them leeway to do anything they want with that information. And they have privacy policies that impose limits on how they can use that data. But there's no simple answer as to whether the information belongs to me or to the site."

Wharton management professor [Stephen J. Kobrin](#) says he is not sure that "Who owns you?" is the right question. "It seems there's just so much information out there about all of us that it's all in the public domain. It may not be there legally, but there's so much in so many places and there are so many ways to aggregate it, that it may not be a reasonable question. The real question is: 'Is it possible to provide some protection to individuals to prevent everything about them from going to everyone else? And, if it is possible, how can you do it?'"

Postcards, not Letters

Kendall Whitehouse, senior director of information technology at Wharton, says some of the key questions raised by the growth of Internet usage go to the heart of the issue of privacy: "What is your expectation of privacy and is it valid? Are people aware of just how wrongheaded their expectations of privacy probably are?"

When it comes to an email message, for example, people tend to think of it as a private correspondence written to someone else, similar to a letter in a sealed envelope. But an email message is more like a postcard, according to Whitehouse. "Your mailman can read your postcard -- by chance, by design or because he's bored. The administrator of an email server is like the mailman; an email message is just a file on the server. Most administrators have no reason to look at it. But it's there nonetheless. And let's say you delete your email. Is it gone? It's gone from some places, but it could be backed up by the Internet service provider. How long will it be held? Electronic documents are like kudzu: They can be hard to eradicate."

Susan Freiwald, a former Wharton faculty member who now teaches cyberlaw at the University of San Francisco School of Law, says the legal community has been debating for years whether it is more appropriate to view personal information as a form of property that is "owned" and therefore subject to property protections, or to look at personal information as a privacy right. Over time, the privacy-rights model, not the property model, has emerged as the prism through which courts view rights to personal information.

"The ownership model hasn't taken off in the law," says Freiwald. "The basic idea in law is that someone who gathers the information owns it, whether it's you [who gathers it] or not." For instance, courts have generally rejected arguments by litigants who have challenged the ability of credit card companies to use personal information on the grounds that the litigants "owned" information about themselves.

In Freiwald's view, however, privacy law remains largely uncharted waters in affording protection to individuals. "Our legal system does a much better job protecting property interests rather than dignity interests, such as privacy," she says. "You can draw that conclusion by looking at the penalties we impose on people for stealing intellectual or tangible property versus for violating privacy. The law is not protecting personal privacy very well." When courts do find privacy violations, she says, the penalties are low.

There are, Freiwald explains, limits to what one can say or post on the Internet without running the risk of being sued successfully. One limit is making money off the fame of someone else, such as a celebrity. Another is identity theft and using credit information to make purchases. So, what legal recourse would be available to someone who felt they were defamed by something posted on the web, like the Korean woman who suffered humiliation in the dog-mess case? Not much, says Freiwald, since truth is an absolute defense against defamation.

An individual can sue someone for public disclosure of private fact. But people who are members of MySpace, Facebook or other social-networking sites are taking a big chance by posting intimate information about themselves. For one thing, the sites generally disclaim liabilities for postings. Moreover, it would be hard for people to convince a court that they were harmed by photos or information that they themselves posted or by true information about them posted by others, according to Freiwald.

"What gets in the way of people bringing claims over information on the web is that it's hard to claim the information is private; it [would have to be] highly offensive," she says. "The more we get used to salacious information coming out about people, the harder it is to establish that the information posted about you can be [considered] highly offensive. We want norms to be kept up with, and norms are changing."

Even the lowly email carries enormous risks. "We have a well-entrenched notion of the assumption of risk," according to Freiwald. "If I send you an email and you forward it, I've taken the risk that you were going to do that by sending you the email. If I send the email, the law considers me taking the risk."

A Declining 'Taste for Privacy'

Allen, who is writing a book on people's "taste for privacy," says the general erosion of privacy today -- more often than not willingly relinquished by Internet users -- troubles her. If the amount of privacy desired by society at large could be ranked on a scale of one to 10 -- with 10 representing a strong taste for privacy -- she would rate it a four.

"What worries me the most is that individuals are growing increasingly insensitive to their own privacy interests," Allen notes. "I think a lot of problems we're seeing have to do with the indiscretion of individuals when it comes to giving people personal data about themselves. I worry about the loss in the taste for privacy as well as the loss of respect for privacy.... [People are] willing to put naked pictures of themselves on the web. They do all kinds of things they regret."

Many young people hardly seem to worry about Internet privacy questions. Wharton's Kobrin tells a story about a panel discussion at the World Economic Forum in Davos, Switzerland, a few years ago. The subject of privacy and information sharing arose, and the young editor of a high-technology magazine said, as Kobrin recalls it, "Only people of your generation are worried about this stuff. We take it for granted."

But with all of the information available about people on the Internet, even Allen feels employers have a responsibility to use Google to check for information that might reflect on the character of job applicants. Indeed, Allen, in the process of performing her duties on boards of directors, has googled applicants seeking positions and has "found information about people that caused me to change my views about their suitability for employment."

Carol R. Freeman, a partner who specializes in labor and employment at the law firm of Morgan, Lewis & Bockius in Palo Alto, Calif., says personal information on the Internet raises a number of questions related to the employer-employee relationship. The law clearly addresses some but not others. For instance, to what extent can an employer rely on information that it discovers on the Internet in making decisions about hiring, disciplining or terminating employees? About 30 states have laws protecting lawful activity outside of work, such as smoking and consuming alcohol.

"If an employer is looking to hire someone and finds a website such as MySpace that discusses how that person gets drunk every weekend, the law is not clear whether that is [evidence the employer can use] in deciding whether to hire the applicant," says Freeman. "The law says you can drink. However, the law does not address the judgment of someone who posts such information about himself or herself. What if the applicant indicates that he is an alcoholic? Then, the employer needs to consider whether there are any implications under state and federal disability laws."

Or, if the operator of a day-care center has a 22-year-old employee who writes about smoking marijuana on a personal blog, should the operator be able to fire her? "The day-care operator in this situation should consult with counsel familiar with the laws in which the day-care center operates," Freeman says. "But, generally, a day-care operator is allowed to terminate an employee for admitted drug use, even on the employee's own time."

Or consider the example of someone who discloses on a website that she was recently arrested. "For example, under California law, an employer cannot refuse to hire and cannot fire or discipline any employee simply because the employee is arrested, but only if the employee is convicted," according to Freeman. "Therefore, the employer should be careful not to terminate an employee based on an arrest. But, there may be other reasons that the employer can terminate -- for example, unavailability for work."

Employers "need to think about these issues before taking action," Freeman says. "Just because information about an employee is on a blog or a website, employers have to ask, 'Are they doing something that's legally protectable?'"

Rethinking Social Norms

Werbach says privacy is only one way to look at the issue of the amount of information available in cyberspace in what he calls "a world of increasingly universal connectivity." he has written a paper, yet to be published, titled, "Sensors and Sensibilities," in which he examines why the law will gradually evolve to accommodate a radically changed world of not just a burgeoning Internet but of camera-enabled mobile telephones, wireless RFID (radio frequency identification tags) and other sensors that can track individual human activity.

"The reality of today's world is that lots of information is out there, and it gets out there for reasons that often have nothing to do with intentional efforts to convey information about people," Werbach says. He argues in his paper that privacy is not the best lens through which to examine such issues. He says there is a need to rethink entirely what society deems to be norms for behavior. "Privacy is certainly important; there are things that should not be disclosed. But privacy tends to impose a formalistic, hard-edged, legal categorization."

The incident on the Korean subway, for instance, can be viewed in two ways. One can argue that the photographed woman's privacy was violated and her reputation damaged. Or one can say that she was in a public place, and the fact that someone took a picture of her wasn't an invasion of privacy since she was not home behind closed doors, and that she should have realized that actions have consequences. Which is right?

"I don't say I know the exact answer," says Werbach. "But evaluating that case through a privacy lens -- whether she was doing something in private or public -- doesn't help us that much because lots of situations that used to be private are now public. It's not a question of privacy but of social norms. Perhaps the answer is just, 'That's too bad.' If someone had snapped a photo of her robbing a bank and she said, 'You can't take a photo of me,' most of us would say, 'Too bad, you were robbing a bank.' In a perverse way, we're going back to the small town where everyone knows what everyone else is doing by virtue of the global information superhighway. My point is, right or wrong, this is going to happen. Google is not going to go away."

This is a single/personal use copy of Knowledge@Wharton. For multiple copies, custom reprints, e-prints, posters or plaques, please contact PARS International: reprints@parsintl.com P. (212) 221-9595 x407.