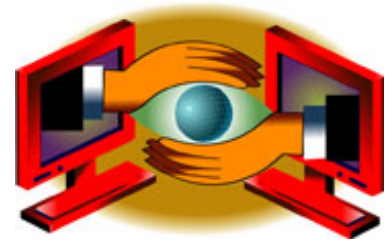




## Nowhere to Run, Nowhere to Hide: The Online Privacy Issue

Published : April 05, 2006 in [Knowledge@Wharton](#)

When Google announced its Gmail email service two years ago, a lot of people figured the company was joking. After all, the press release was circulated on April Fool's Day, and Google had been known to offer up the occasional gag, like saying it was starting a research center on the moon.



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](mailto:reprints@parsintl.com) P. (212) 221-9595 x407.

More importantly, the business proposition seemed preposterous. Nobody believed that consumers would tolerate Google's plan of having its computers scan an individual's emails and then deliver advertisements to him or her based on the emails' contents. Google, of course, wasn't kidding. Two years later, Gmail has tens of millions of users, and the company continues to add new features.

But the incredulity prompted by Gmail's introduction underscores the web's knotty privacy problem, according to participants at the recent 2006 Wharton Technology Conference. Consumers say they want privacy online although they often behave in ways that contradict those statements by, for example, posting intensely personal information and photos on public websites. Companies insist that they will protect privacy, although they sometimes fail to do so. And everybody is wary of increased government regulation; indeed, some people worry more about potential government misconduct than about corporate abuse. "In a world of photo traffic tickets and warrantless searches, what Google does with my personal information doesn't bother me," quipped conference panelist Gil Brodnitz, a partner at Accenture.

Debating online privacy isn't merely a philosophical exercise. Companies collect reams of information about visitors to their websites and about their customers' web-surfing ways. You may be able to hide your visits to offbeat, or off-color, websites from your spouse, but you can't hide them from Google and Yahoo. And governments at all levels have shown an increasing hunger for that kind of information. In March, for example, Google squared off with the U.S. government in two privacy cases. In the first case, a judge ruled that the company must give the Federal Trade Commission the entire contents of a customer's Gmail account, including deleted messages. In the second, a judge said that the company had to provide 50,000 web addresses from its database to the Justice Department for a study of child pornography online. In a victory for the company, however, the judge in that case rejected the government's demand for keywords used by customers in searches.

### "Rights to Content in Perpetuity"

In the absence of clear federal rules, web surfers cannot be guaranteed that firms will protect user information, said conference panelist Wendy Seltzer, a visiting professor at the Brooklyn School of Law. In the pornography case, for example, while Google chose to resist the government's subpoena, Yahoo, AOL and MSN complied. "If we don't have a strong protection law, all we have is the company's word, and hype and fact don't always match," she noted. "Anything that is collected in a regime of weak privacy laws is something that the government can get access to."

Even so, many companies, especially high-profile web pioneers, are trying to stake out positions as responsible stewards of their customers' information. "We try to be extremely explicit about the data we are collecting and how we are storing it, and we let the customer know the benefits to them," said panelist

Bradley Horowitz, head of technology development for Yahoo's search and marketplace group. "We let them know that if they are willing to let us target ads to them, they will get more relevant content. If we are vigilant and explicit," users can make decisions that best meet their needs.

But even the most conscientious firm sometimes stumbles. Yahoo, for example, came under criticism when it changed the terms of the user agreement at its Geocities division, said panelist Declan McCullagh, who covers online privacy for CNET News.com. The company "was claiming rights to all of your content in perpetuity. It was remarkably broad. It was just the work of an overzealous lawyer, but it allowed competitors to say, 'We are not going to make movies based on your content. Come to us.'"

Despite this incident, McCullagh suggested that most complaints about privacy problems on the web come not from consumers, but from "the privacy fundamentalists -- the pro-regulation privacy groups -- and the politicians, who are always trying to get their names in the newspaper." After Google introduced Gmail, for example, a California lawmaker introduced a bill to ban the service. McCullagh argued that consumers accept existing safeguards as long as they believe they are getting better prices or programming in return for relinquishing personal details.

Panelist Steve Johnson, chief executive of Cambridge, Mass.-based Choicestream, which makes personalization software for websites, agreed. "There is a simple divide in the world of consumer profiling -- the type consumers like and the type they don't. Consumers don't like it when they have no control, when they are being watched with so-called spyware or when they can't opt out. But they like it when they can see that data can be opted out of and when the watching is done by a trusted source like Amazon or iTunes."

In addition, consumers are less likely to try to disguise their identity by lying about themselves in site registrations if they believe that their details will be used to serve them, he said. "With The New York Times, if you are willing to share personal information, you get the most relevant book reviews. So you don't have any incentive to spoof it." In many cases, spoofing is futile anyway, argued panelist [Ravi Aron](#), Wharton professor of operations and information management. Companies that track web-surfing behavior can quickly build demographic profiles of users based on the sites they visit and the services they use. "Providers can tell if you are spoofing if you say you are an 85-year-old grandma and your behavior doesn't match the stuff that an 85-year-old grandma would read," he said.

### Accepting Privacy Tradeoffs

In some ways, the debate over privacy on the web shows amnesia about longstanding business practices and consumer behavior, said Accenture's Brodnitz. "People have been trading personal credit information for better rates on loans for years. They will give up information in exchange for higher quality or good service. Capital One broke the back of the 19.1% interest rate on credit cards by looking at other kinds of information."

And even before Capital One, financial-services firms had large amounts of data on their customers' incomes, debts, purchase histories and personal preferences. A credit-card issuer knows, for example, the places its customers visit and the sorts of restaurants they favor. Consumers, in essence, invite hefty invasions of their privacy for the convenience of the cards.

Brodnitz also suggested that companies fret too much about the potential downsides of protecting privacy. They worry, for example, that most customers might reject being marketed to based on their personal information. But consumers, he pointed out, like the idea of privacy more than they like to ensure the protection of theirs. "Everybody wants a privacy policy, but nobody wants to read it. What companies need to realize is that people want the ability to opt-out even if they never do it."

Privacy protection isn't just an obstacle to making money, Brodnitz added. It also presents opportunities.

Companies that already occupy trusted positions, like brokerages and law firms, might present themselves as protectors and brokers of private information. Consumers might authorize them to make judgments about when and to what extent personal information should be released.

But these sorts of businesses may not emerge unless federal lawmakers clarify the muddle of privacy protections in the United States. If anything, the current crazy quilt of laws can make business more costly, said Brooklyn Law School's Seltzer. "We don't have an overarching data privacy law, and companies therefore have to contend with a patchwork of federal and state laws."

Just at the federal level, companies must grapple with a variety of rules that protect privacy to differing extents. "Health care information is strongly regulated under [the Health Insurance Portability and Accountability Act]," Seltzer noted. "Financial information has some protection, and the [Federal Trade Commission] can go after unfair and deceptive trade practices." For example, ChoicePoint -- a Georgia-based provider of identification and credential verification services -- "settled with the FTC for \$15 million, including \$5 million in restitution to customers, for a security breach."

Without a federal privacy umbrella, individual cases mainly boil down to contracts. The ownership of a person's online profile -- that is, her identity and web-surfing behavior -- and a company's ability to use it depends on the user agreements that she accepts when registering for sites. "People should be careful in signing up for these things," Seltzer warned. Provisions accepted unwittingly can come back to haunt them.

U.S. online protections, rudimentary as they may be, are far ahead of those in some parts of the world, especially developing markets like India. India, of course, has become a major locale for information-technology outsourcing, which means that some consumer data will inevitably end up there. And it's not clear what redress U.S. consumers might have if their personal information were released in, say, Bangalore.

"That has the potential to be a political issue," CNET's McCullagh acknowledged. "Data leaks can happen anywhere. But as long as a country has a functioning legal system, you should be able to put the issue in your contracts."

---

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](mailto:reprints@parsintl.com) P. (212) 221-9595 x407.