



Protecting privacy

[Chuck Miller](#)

June 01 2009

<http://www.scmagazineus.com/Protecting-privacy/article/137626/>

Consumers are willing to offer up personal information, provided they recognize a specific benefit for that interaction, reports Chuck Miller.

New technology brings new challenges, especially when it comes to privacy. In the old days, it seemed easier to keep personal financial and identity information secret. If a company had information about its clients, it could be kept locked away in an area guarded by fences and dogs.

Few companies today can exercise that kind of discretion. In a world of interconnected databases, worldwide computer networks, and billions of transactions taking place every second, how can confidentiality be preserved? And how can an enterprise live up to expectations of security and mandates to preserve the privacy of the data it holds on millions of customers?

Enterprises, too, must worry about more than direct financial impact. In the past, companies thought that insurance policies could protect the enterprise from financial jolts due to loss of data – but now these entities are faced also with loss of reputation, which insurance cannot effectively protect.

“How do you prevent your enterprise from having reputation damage or loss of consumer confidence because of data breaches or bad privacy practices? These bleed together,” says Mark Cohn, vice president of enterprise security at Unisys.

One of the reasons so much data is captured, seemingly at every turn, is that having it online makes it much less expensive for enterprises to interact with customers. That is, usually -- to the enterprise – the drivers are cheaper information provision and even cheaper data capture.

“Going from face-to-face tellers, to ATM, to internet banking – each one of those steps reduces cost by an order of magnitude,” says Cohn. “But if there are problems because of data breaches or other factors, then cost could actually go up.”

Ideally, if privacy can be thought of as hiding information about one's self, then the sharing of that information should be selective and controlled. And consumers are increasingly aware of the consequences of having their personal information widely and readily available. Many fear providing it unless they see a real benefit.

“Privacy concerns to a significant number of people are major factors in whether they are comfortable with a consumer-facing website,” says Cohn. “As companies try to reduce costs by moving more operations to automation, the consumers' willingness to go along determines whether the companies can get the benefits they would like.”

Thus, privacy may be voluntarily sacrificed, normally in exchange for perceived benefits. Cohn pointed out that in Unisys surveys, people say they are willing to provide personal information if it streamlines their interactions and provides some kind of benefit.

“You have to associate providing personal information with a specific benefit for that interaction. And you want to provide an assurance of what the information will be used for, and that the user will have control over whether it will be used for other purposes,” Cohn says.

Compliance issues

Another factor in trying to protect privacy is how best to comply with regulations set up to protect personal identifiable information.

It doesn't help that much of the data about people is sliced and diced, mined or even sold to third parties. Such information could potentially be used for purposes not known to the individual providing the information.

Privacy concerns exist wherever in the world uniquely identifiable data relating to a person is collected and stored. The origin of identity is always government-based. If someone is hired by a company, the first day on the job they will be asked for a driver's license or something else issued by the government to establish identity.

The federal government has mechanisms and agencies in place to ensure the public's privacy protection, including the Federal Trade Commission (FTC), which claims that privacy is a central element of its consumer protection mission. But even the FTC cautions that as personal information becomes more accessible, companies, associations, government agencies and consumers alike must take precautions to protect against its misuse.

The call for stricter regulations could help motivate increasing numbers of enterprises to participate in a movement to better protect individual privacy.

“In the United States, stringent regulations could be a wake up call that says we need a

comprehensive understanding and a plan on how to deal with information privacy,” says Rob Marano, president, CEO and CTO of InDorse Technologies. “But it is not going to happen anytime soon. In the meantime, the wakeup call could be a data breach that causes a company to wind up on the front page of *The Washington Post*.”

In other parts of the world, privacy is seemingly taken much more seriously than in the United States. “The data privacy laws in the European Union are very strict,” says Marano.

Can it be that the problem is just too intractable?

“Data loss may be controlled, but it probably cannot be stopped entirely,” says Marano. “And since much of the problem is based on human behavior, to fix it you have to change behavior. Thus, it will be impossible to fully contain. The challenge to the industry is to enable users to be safe online, but without having to go through a lot of change.”

Locking IDs

In this economic climate, the atmosphere is rife with internal threats. For example, if a disgruntled employee is laid off, they may retain their access to sensitive systems.

“We see this as a major driver leading companies to adopt strong authentication products,” says Thorsten George, vice president of marketing at ActivIdentity. “It is very labor-intensive and expensive sometimes to decommission passwords. You cannot just push a button and decommission thousands of accounts.”

Before an enterprise contemplates privacy assurance or compliance, it is important to know what data it has and how it is being used. In many cases, companies say they do know, but in reality, oftentimes, they do not.

“Companies must go through a data classification process to determine what they have, and determine what it is that is most critical,” says Glen Kosaka, director of data protection marketing at Trend Micro. And then, he adds, they need to find out where it resides and how it gets used.

In some cases, that means reference to how data is collected, stored and associated. In other cases, the issue is who has access to the information. Other issues include whether an individual has any ownership rights to data about them, and/or the right to view, verify and challenge that information.

The next step is to determine the most vulnerable leak vector. Is it laptops, desktops, offshore sites, USB storage, email? Typically, the highest priority vectors are email, laptops and removable storage devices. And as iPhones and MP3 players become more popular, more ways for data to leave the company – either accidentally or maliciously – are introduced.

The bottom line is that protection of privacy requires constant vigilance and enterprises are likely to be the primary targets for those who would invade it.

“No security solution is perfect,” says Trend Micro's Kosaka. “A determined thief can always find a way to get around the system.”

[sidebar]

ONLINE PRIVACY: A look back

The basis of governmental protection online goes way back, and includes measures passed by Congress such as:

- The Fair Credit Reporting Act (1970)
- Privacy Act of 1974
- Family Education Rights and Privacy Act (1974)
- Right to Financial Privacy Act (1978)
- Privacy Protection Act of 1980
- Cable Communications Policy Act of 1984
- Electronic Communications Privacy Act (1986) Video Privacy Protection Act of 1988
- Telephone Consumer Protection Act of 1991
- Driver's Privacy Protection Act of 1994
- Communications Assistance for Law Enforcement Act of 1994
- Telecommunications Act of 1996
- Health Insurance Portability and Accountability Act of 1996
- Children's Online Privacy Protection Act (COPPA) of 1998
- Financial Modernization Act (Gramm-Leach-Bliley Act) (2000)