



Do You Know Where Your Identity Is? Personal Data Theft Eludes Easy Remedies

Published : April 20, 2005 in [Knowledge@Wharton](http://knowledge.wharton.upenn.edu/article.cfm?articleid=1176)

ChoicePoint, a consumer data vendor, hands over personal information on at least 145,000 people to criminals posing as small businesses. Hackers swipe the personal information of 32,000 people who use the database Lexis-Nexis. Bank of America loses backup tapes containing 1.2 million federal employee records. Every day, it seems, a new identify theft incident is reported (or occurs, without being reported) followed by new rounds of questions: Should data vendors be regulated? Can identity theft hurt e-commerce? How do individuals protect themselves? Unfortunately, suggest Wharton faculty and others, no simple answers are available, especially when personal information is so easily available through search engines.



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.

The cost of identity theft continues to escalate. According to a Federal Trade Commission survey released in September 2003, the latest year available, nearly 10 million Americans have been victims of some form of identity theft, resulting in \$47.6 billion in damages accruing to businesses. Victims spent an average of 30 hours trying to fix the damage and suffered losses totaling \$5 billion.

Those figures are likely to grow in the future, given the number of incidents reported so far this year. In addition, because a recent California law requires any company that operates in the state to disclose when personal information is lost, incidents continue to surface at a rapid clip: On March 8, for example, DSW Shoe Warehouse reported the theft of purchase information and credit card numbers from shoppers at 103 stores. Separately, California State University at Chico disclosed that hackers lifted personal information, such as names and social security numbers, from a housing and food service information system.

"Without that California law, we would not have heard of any of these breaches," says Kendall Whitehouse, senior director of information technology at Wharton.

Meanwhile, Senator Diane Feinstein, Democrat from California, proposed a bill on January 24 that would require companies nationally to disclose when customer data has been breached. Modeled after California's state law, the bill was proposed in the last Congress, but never made it into law, says Howard Gantman, director of communications for Feinstein. This time, he adds, "we are hopeful of passage." Indeed, notes Wharton operations and information management professor [Eric Clemons](#), the bill stands a good chance of getting through because of the increasing incidents of identify theft and the public's frustration with the fallout. "You must have recourse against the people responsible for the theft," says Clemons. "There has to be data responsibility."

At the same time, some observers worry that a law targeting firms that peddle data could end up restricting commerce. John A. Greco, Jr., CEO of the Direct Marketing Association, noted in a statement that "a delicate balance must be struck" to prevent identity theft, yet allow customers of data vendors to get information needed to issue credit, verify data and process transactions quickly.

Others, however, predict that better security won't hurt the speed of commerce. If anything, says Wharton legal studies professor [Dan Hunter](#), a decrease in identity theft will actually help commerce. That's

because as companies increasingly disclose data breaches, identity theft may start to hinder online purchasing. "The spate of ID thefts is hardly likely to convince my grandmother that she really needs to start buying online," says Hunter.

But for now, consumers are not yet annoyed enough about identity theft to push for tighter regulation. Consumers see identity theft as "just one of those things," says Hunter. "As long as it doesn't happen to them, they assume it won't."

The Need to Disclose Breaches

According to Clemons, the security breaches at ChoicePoint and Lexis-Nexis could tip the scales in favor of Feinstein's bill. Indeed, while Clemons initially wasn't in favor of a national law on identity theft disclosure, he now believes one is necessary. Without a law forcing disclosure and/or penalties for data leaks, companies aren't going to worry about protecting data, he suggests. Why? Because companies that currently leak information aren't responsible for damages. Financial institutions pick up most of the tab for bank fraud, stolen credit card numbers and the like. "If 100% of the damages were paid by the guy who allowed the data to be stolen, there would be a different attitude about security," says Clemons. "Disclosure makes sense, and some financial sanctions would probably be appropriate as well."

Hunter agrees that a law is necessary, but notes that legislation will have a tough road given resistance from marketing companies that rely on building profiles for their business. And companies like ChoicePoint, which are largely unregulated today, are not going to welcome laws governing their security policies. In addition, Hunter says, attitudes about personal data integrity need to change. "We have this bizarre idea that data collected by companies is their 'property' based on the theory that they collected or bought it. Therefore, they can do what they want with it. Yet if we took a moment to recognize the sorts of social and individual costs that entirely blameless people have to bear when their identity is stolen, we would institute higher standards on security, access and editing of people's personal identifying information."

Clemons says a national law is warranted for three reasons: First, identity theft is becoming financially significant and a matter of grave concern to consumers. Second, disclosure gives individuals and their financial institutions time to protect themselves and can provide fair warning for these parties considering that the bulk of the financial risk is carried by them. Indeed, Whitehouse notes, giving consumers time to react to identity theft is one of the biggest reasons to pass Feinstein's law. "I think consumers need to be informed quickly," so they can "report the theft to credit agencies and thereby minimize the risk of danger. Without disclosure you only find out when the fraud happens. That's too late."

Third, there is no downside to disclosure aside from the embarrassment suffered by companies that have to admit leaks. A disclosure law would at least reassign some of that risk by tarnishing the reputation of the parties that either caused the damage or allowed it to occur.

For example, since ChoicePoint's security problems surfaced, the company has exited a business selling data such as Social Security and driver's license numbers unless there is specific consumer-driven transaction or benefit, or unless the products support federal, state or local government and criminal justice purposes. ChoicePoint has also appointed Carol A. DiBattiste, currently deputy administrator of the U.S. Transportation Security Administration, to be the company's chief credentialing, compliance and privacy officer. "These changes are a direct result of the recent fraud activity," said ChoicePoint CEO Derek Smith in a statement.

Identity Theft: Easy and Often

So why does identity theft seem like a snowball rolling downhill? Because it's so easy. Once personal information hits the Internet, it doesn't go away. According to Hunter, a little time spent on Lexis-Nexis can turn up property records, taxes paid and other personal information. "Until we recognize that

personally identifying data is valuable as an aspect of an individual's life, not just as part of the bottom line of companies like Reed-Elsevier (the parent of Lexis-Nexis), we are going to wake up to a new violation approximately every three days," says Hunter.

But the real issue is, who needs a Lexis-Nexis account when Google is available? Joshua Pennell, CEO of IOActive, a Seattle-based security company, was recently at a law enforcement conference illustrating how easy it is to find personal identifiers using Google. "With Google, it doesn't matter if you are an evil hacker," says Pennell. "Anyone can do it." He turned up more than 1,000 records, in addition to such documents as corporate personnel reviews, Excel spreadsheets and scanned passports. How did this data get to the web? Companies, or individuals, put the documents there assuming no one would see them. "What we have here is a cultural issue," says Pennell. "You can have all the firewalls in the world, but if you post documents on the web they will be seen. Security is lax."

That's why Pennell says a law could boost security. "To bring cultural change, we are going to have to make companies air dirty laundry. Who wants to tell the world they lost your information?"

David Farber, a former University of Pennsylvania professor of information science who is now at Carnegie Mellon, says the Internet makes it easy to pick up little bits of information and piece them together to assume someone's identity. Personal data on the web is like the genie that won't go back into the bottle. "The fact that we are living in a networked world makes this a lot harder to deal with," he says.

Fixing the Problem

Because identity theft is a) easy, and b) the result of lax corporate procedures, consumers and companies with personal data have to meet each other halfway to prevent ID theft, says Farber. "Corporate procedures need to be changed, and consumers have to watch their data." On the consumer side of the equation, Farber echoes many others who have advised individuals to shred documents and refrain from giving out personal information. He uses one credit card for online transactions so that he has to cancel only one when his security is compromised. He also doesn't respond to emails asking for information such as credit card and Social Security numbers, and he checks credit reports regularly.

Until either data aggregators become more secure, or legislation forces companies to be more vigilant about data, the onus is on the consumer to protect personal data. Clemons says if a consumer gives out just one nugget of information, a thief can build on it. "A thief can use simple, readily available information like a Social Security number, phone number or parent's name to establish" an identity, and "then get increasingly more sensitive information very easily."

On the corporate side, it's unlikely there will be much movement without regulation on the federal level, Clemons suggests. Why? In the absence of penalties tied to data mishaps, there's not a big return on investment to justify beefing up security. "There was no return on investment on pollution control until legislation and litigation reassigned much of the cost of pollution back to the pollution creators," says Clemons. Similarly, investments to "plug holes" will be made "the first time that a data aggregator is assessed the full financial damages caused to banks and credit card issuers by its failure to protect data." In economics, the current setup for data aggregators is known as an "externality," says Clemons. "One party enjoys the benefits while another bears the costs."

Technology as Magic Bullet?

Although technology has arguably made identity theft easier, can it also be better used to secure information?

Not really, says Whitehouse. The key to protecting identity is building a system with multiple layers of security. To get to data, someone should have to go through tiers of security procedures. Adding more security would require two things: Consumer acceptance and new procedures for financial transactions.

The rub is that this solution isn't popular, especially if, for example, it takes a little longer to get credit approved. Clemons explains that something as simple as losing a password would become more inconvenient. "Since it would be harder to establish that you are you, it would be harder to establish your right to your password," he says.

Other solutions would be to no longer use Social Security numbers as identification, to frequently change passwords and to use virtual credit card numbers that change with each online purchase so that real numbers aren't revealed. If all of those solutions are integrated with information systems, the value of leaked data approaches zero, says Clemons.

Since those solutions aren't going to happen overnight, consumers are left with little to ease their pain, except maybe a prayer that their identity isn't stolen, says Hunter. "This area is a genuinely filthy can of worms. And it's not going to get better anytime soon."

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.