

[Email this article](#)
[Print this article](#)
[Most popular pages](#)

[Click to send](#)
Choose File Print or Ctrl P or Apple P
[Today](#) | [This Week](#)

Data vulnerability is a systemic problem

Torin Monahan
Arizona State University
May. 21, 2006 12:00 AM

Identity theft now represents the largest category of fraud-related complaints in the country. According to the Federal Trade Commission, 255,000 identity theft complaints were filed in 2005 alone.

These include things like credit-card theft, illegal wire transfers, Internet scams, phone and utilities fraud, and theft of business data. Notably, Phoenix tops the FTC list with the highest number of reported identity theft complaints per capita in the country.

Police departments have responded to this new crime threat by launching coordinated public education programs to teach consumers to protect themselves better. Some police recommendations include buying paper shredders for home use, shielding the keypad when using an ATM, not disclosing any personal information over the phone or the Internet, and setting up network firewalls to safeguard electronic data.

Indeed the general law enforcement response to this rapidly growing crime category is to push responsibility onto individuals (or victims) to protect themselves. Although self-protection is crucial within today's climate of data vulnerability, this approach neglects the vulnerabilities of a system that catalyzes identity theft in the first place.

The very technological systems that streamline communication, commerce and trade also open us up to intrusive forms of electronic surveillance, whether by identity theft criminals or by the National Security Agency. This is a point often overlooked in discussions of electronic monitoring or crime.

Because we haven't had a genuine public debate about the kinds of technologies we see as necessary to adopt, or about the important safeguards that should be implemented for the preservation of social goods (such as crime prevention or privacy), vulnerable information systems multiply.

In effect, individual consumers or employees are blamed for their own victimization. But the systems or the industries that make people such easy targets are seldom re-evaluated. These systems are the massive databases of consumer information that are stockpiled by credit agencies, telecommunications companies and are targeted for advertising and lucrative sharing arrangements among companies.

To question the necessity of these systems would not just challenge ideas of technological progress, it would threaten the profit quest of information industries.

Nonetheless, information industries are the very ones undermining our data security and increasing our vulnerability to identity theft. Just to put things into perspective, while hundreds of thousands of complaints may be filed with the FTC each year, millions of data records are compromised.

In one of several recent high-profile cases, 40 million credit cards were compromised when hackers penetrated the database of CardSystems Solutions Inc. in Tucson in 2004.

Such cases can occur because of vulnerable information systems and their companies.

The fact that industries poorly manage their networks, fail to ensure proper encryption, share data liberally and maintain records far longer than is necessary compounds the problem.

The most egregious cases of identity theft are not the fault of individuals, whether victims or criminals; they are the result of information systems and industries out of control and in sore need of serious regulation.

The FTC can fine companies that have not taken reasonable precautions to ensure confidentiality of consumer data. Notwithstanding the potential for fines to galvanize better data protection by companies, this Band-Aid approach to regulation is ultimately insufficient.

It doesn't address the problem of data stockpiling and exchange among companies. It doesn't call for the redesign of information architectures to ensure anonymity and confidentiality at every step of the way. Most importantly, it bypasses the pressing need in the United States for serious data protection laws, the likes of which do exist in other countries.

We could, for example, presuppose that everyone opts out of data sharing by default. Currently, it is almost always the opposite: Everyone is opted in for data sharing, forcing individuals to contact credit companies and others to request that his or her information isn't shared.

This opt-out default could be legislated, making all of us less vulnerable to identity theft. Similarly, we could have clear guidelines for who has access to our data, how it can be shared and when it will be destroyed.

Until we are willing to address data vulnerability as a systemic problem, rather than as an individual one, identity theft will continue to increase and exceed our capacity for dealing with it.

Torin Monahan is an assistant professor at the Arizona State University School of Justice & Social Inquiry.

[Email this article](#)
[Print this article](#)
[Most popular pages](#)

[Click to send](#)
Choose File Print or Ctrl P or Apple P
[Today](#) | [This Week](#)