

## WHEN DOES A PRIVACY BREACH CAUSE HARM?

**Jay Cline**  
**March 06, 2008**

Several countries are on the verge of doing what U.S. courts have stopped short of: codifying that breaches of personal information can actually harm people. Why should U.S. companies welcome this development?

Because an international answer to this question could clarify the standard of protection that corporations have to meet with regard to personal data in their care. Finally having a clear standard could contain corporate liability and reduce companies' operational expenses. Whether the U.S. Congress also makes this leap in its deliberations over a national breach-notification bill may depend on legal experts stepping up to the plate to reshape the terms of the debate.

Let's face it: U.S. courts have botched this one. Time and again, when plaintiffs have sued companies for exposing their personal data, the only damages courts have awarded them, if any, have been for monetary losses relating to account fraud or identity theft.

On the one hand, most large data breaches don't even lead to a rash of ID thefts. As forensics firm [ID Analytics Inc.](#) has shown in a number of case studies, lost laptops and other similar breaches involving thousands of people's sensitive information resulted in only about a dozen verifiable instances of fraud.

But is monetary loss the only criterion for personal harm? Anyone who has experienced true ID theft would say the money is only a part of the equation. The countless obstacles to getting on with life, not to mention the psychological dread, can outweigh the hard-dollar losses.

So when do privacy breaches cause harm? That's what I asked Anita Allen, a professor at the University of Pennsylvania's law school. Allen is scheduled to address this topic later this month at the [International Association of Privacy Professionals Summit](#) in Washington.

"Identity theft and financial fraud are one sort of harm," Allen said. "But others include offensive publication of illicitly acquired personal information, along with hurt feelings and dashed expectations. The assault on personality and feelings is the quintessential privacy injury."

To that end, we can all think of examples in our own lives where privacy exposures harmed us or people we knew. Predators who exploit information about children online, forwarded e-mail chains that damage relationships and compromising photos sent by cell phones are three examples that come to mind.

But what about the information potentially obtained by insurance companies and employers that could limit someone's economic possibilities, or information obtained by government agencies that threaten our sense of autonomy? These can all harm our human dignity.

U.S. courts have been reluctant, however, to award tangible dollars for these intangible harms. We can hardly blame them for reflecting American philosophical prejudices. We primarily define our individual rights in relation to the government, not industry. We also define the person in terms of his material body, but give short shrift to the intangible mind and soul that even the ancient Greeks accepted as components of the whole person. Our materialist individualism chains down the judge's gavel.

The tide may be turning. Other countries watching the U.S. experience with security-breach notification are feeling pressure to extend these same privileges to their citizens. Last summer, Canada and New Zealand issued guidelines for security-breach notification. The U.K., European Union, Australia and South

Africa are considering similar laws. The privacy commissioners of Canada, Australia and New Zealand have voiced support for notification when there is risk of harm to the individual.

Their goal of setting a harm threshold is almost certainly intended to avoid the major shortcoming we've had in the U.S.: overnotification. Companies operating in the U.S. now feel compelled to notify people of every lost backup tape, regardless of whether the tapes might turn up in a month or if a thief could even make sense of the data on the tape. Foreign countries don't want to impose that kind of unnecessary cost on their companies.

But in the process of defining thresholds for privacy harm, either in legislation or through their case-by-case enforcement of the laws, these countries could be doing the world a big favor. They could be exporting a rejuvenated conversation to U.S. shores.

Do I expect to see these deeply ingrained aspects of American society change anytime soon? Not really. But as we enter an era of greater use of radio frequency identification, DNA databases, portable medical histories, Global Positioning System data and improved antiterrorist tracking technologies, the personal consequences -- and political pressure -- of data breaches will only increase.

*Jay Cline is a former chief privacy officer of a Fortune 500 company and now president of [Minnesota Privacy Consultants](#). You can reach him at [cwprivacy@computerworld.com](mailto:cwprivacy@computerworld.com).*