

# Top Privacy Developments for Global Corporations

Jay Cline

May 15, 2006 ([Computerworld](#))

A record-setting 800 privacy professionals attended the latest International Association of Privacy Professionals conference, and it's no wonder: The privacy issues facing multinationals have only increased over the past year. From security breaches to data retention, the privacy role has expanded into new areas of many businesses. Companies that had relegated privacy to a part-time position in the legal department are having second thoughts about how to combat these new million-dollar risks.

Here's a global roundup of the main developments:

## United States

- **Security breaches.** Over 80 companies, government agencies and universities experienced publicized security breaches during the first four months of 2006, up from 30 during the same period in 2005, according to [privacyrights.org](#).

Over 11% of Americans surveyed late last year by Ponemon Institute LLC (on behalf of law firm White & Case LLP) received a letter informing them of a possible breach of their information. This increase, fueled by new state laws on security-breach notification, has added a new project to privacy officers' agendas: upgrading their incident-response process.

- **Employee monitoring.** Long told by the information-security profession that employees are the biggest source of security breaches, three-fourths of American employers now monitor employee Internet use ([download PowerPoint presentation](#)), and half review employee e-mails and computer files. As a result, Gartner Inc. is forecasting that the nascent content-filtering market will double in 2006 ([download PDF](#)). What's the impact to privacy leaders? Higher need to communicate company policy to employees, and more incidents to respond to.

- **FTC enforcement.** Over the past year, the Federal Trade Commission settled five major cases against U.S. companies for insufficient information security, including a \$15 million fine for ChoicePoint Inc. As a result, chief privacy officers (CPO) are spending more time with their information-security counterparts learning about laptop encryption and wireless-access points.

## Europe

- **Data retention.** In February, the European Council adopted a directive requiring companies to retain communication data for at least six months, but possibly 24 months, depending on member-state implementation. The move was intended to aid law-enforcement efforts to track terrorists, but privacy advocates cried foul because of the potential increase in exposure of personal information. Privacy leaders are caught in the middle.
- **Binding corporate rules.** European data commissioners began approving BCRs as another mechanism for companies to legally transfer data out of Europe. But it's a time-intensive process, requiring CPOs to present their companies' privacy policies in the capital of every European country from which they export data. The attention on BCRs has renewed privacy leaders' focus on how their companies are doing managing their European data.
- **Whistleblower hot lines.** Privacy leaders in some U.S. multinationals found a new project on their plates when the European Union moved to prohibit the type of anonymous whistleblower hot lines that U.S. companies had established to comply with the Sarbanes-Oxley Act. Anonymous reporting on neighbors reminded Europeans too much of the abuses of World War II, and not of courageous whistleblowers. The dust-up led observers on both sides of the Atlantic to realize that their differing approaches to privacy were based on different cultural realities and would probably have to co-exist for years to come.

## Other

- **Security breaches.** Newspapers in Japan and Canada have shone a continuing spotlight this past year on companies and government agencies that exposed or inappropriately shared personal information.

- **Registration.** Following the European model, the Argentine data-protection commissioner began requiring companies to notify him of their databases of personal information.
- **National privacy laws.** Mexico, China and South Africa have inched closer toward strengthening or adopting national laws to protect personal information.

What does this all add up to for corporate privacy officers, besides more work? The good news is that this is more of the same. The recent year hasn't brought any new ground-shaking developments that defined privacy in a fundamentally new way. Companies that had based their privacy policies on the Safe Harbor's seven privacy principles didn't have to make any major modifications.

But two things did change. First, the scope of American companies finally paying attention to privacy expanded dramatically. Not only did the attendance at the annual IAPP summit jump by about a third, but by my count, the number of privacy and security conferences in the U.S. more than doubled. The growing demand for experienced, Fortune 500 CPOs pushed the typical compensation package up to \$200,000 for the first time. The varying ways in which privacy is being implemented across the globe have also increased the need for external consultants who are specialists in certain industries or countries.

Second, the privacy function became more interdisciplinary this past year, touching more parts of a typical company's operations. The successful privacy leader of a global corporation can no longer be focused narrowly on law or IT. Managing projects, driving organizational change, engaging employees, re-engineering business processes, understanding cultural differences, helping marketing pros find creative solutions -- as well as being fluent in legal and technology concepts -- have all become part and parcel of the CPO's job description.

What can global corporations do to prepare for the coming year of as-yet-unforeseen privacy developments? I'd say three things: Stay with the horse that got many of us here safely -- a privacy policy based on the Safe Harbor principles. Close your information-security gaps. And

overcommunicate to your employees about privacy and security. The stakes are only getting higher for companies that don't master these basic fundamentals.

*Jay Cline manages data privacy at Carlson Companies Inc., a Minneapolis-based group of businesses in the travel, hospitality and marketing industries. These are his views and not necessarily those of Carlson, and should not be taken as legal advice. Contact him at [cwprivacy@computerworld.com](mailto:cwprivacy@computerworld.com).*