Zero Knowledge conference explores Privacy by Design

Report by Eugene Oscapella

PL&B REPORTS FROM THE Zero-Knowledge Systems Conference, held in Montreal, which tackled the privacy and security issues currently facing business. *Privacy by Design* was an apt title for the conference held in Montreal on 3-5 December 2001.

Zero-Knowledge, whose goals include equipping organisations with software and expertise to manage the security and privacy of corporate and customer information assets, assembled an impressive array of speakers from around the globe to address the issues facing business.

Perhaps the most important message generated by the conference was the notion that "privacy in a box" – technology which resolves all corporate privacy problems – simply does not exist. Instead, the conference pushed the idea that privacy can be enhanced through a combination of technology and effective business practices.

Website management

Michael Weider, CEO of Watchfire, a company that produces website management software, explained how technology can help companies address website privacy. This is no small task, since some companies have millions of web pages spread across thousands of sites. Most companies, Weider argued, fail to comply with their own privacy policies. There is a large gap between privacy policies and website reality that will grow as the size of these websites increases. A company's chief privacy officer (CPO) may develop a privacy policy, but marketing and development teams often build websites that do not reflect these policies.

The current approach taken by many companies, he said, falls into three categories: do nothing, review the site before it is launched, or do periodic spot checks after it is launched. These methods, Weider argued, are slow, ineffective and costly.

Among the solutions he proposed:

- define key data protection standards for website content
- identify responsibility for content
- train content creators
- implement automated compliance measurement and reporting systems that can examine each web page by automated means and generate reports
- integrate compliance tests into the publishing process before the website is launched

An automated compliance measurement and reporting system can automatically examine each web page and generate reports – for example, a data collection report about forms used on a website. Is the collection of personal data secure, does the website contain a privacy statement, what cookies are sent to the computer of the person visiting the site? The process of examining website pages is automatic and continuous. Problematic web pages can be examined manually and the problems corrected.

Privacy vs. Security

Bob Blakely, chief scientist for security and privacy at IBM-owned Tivoli Systems, told the conference audience that society is only in the early stages of privacy technology. Security technologies, on the other hand, have a much longer history, since they have been inherited from the military. According to Blakely, security has failed and will continue to fail, and that since society is in the early stages of developing privacy technology, it should ask the great questions to get the technology right.

Blakely says that businesses view personal information as an asset. There are two types of personal information. The first is that which is necessary, such as the address of a customer to whom goods are being delivered. The second is personal information that gives a competitive advantage, since customer "intimacy" may lead to better service and better business. However, selling the latter type of information may hurt a business if the customer feels that their intimacy has been violated.

Blakely argues that personal information may be business property, but it is the individual's secret. In the eyes of the individual, businesses are culpable if that personal information is disclosed. Even if a business can fend off legal liability for the disclosure, individuals will continue to hold it responsible. Therefore, the interesting aspect of privacy is not what the individual discloses to a business, but rather what happens after the information is disclosed. Will the business look like a concerned friend, a detective, a voyeur or a reporter?

Businesses, says Blakely, must collect and use some personal information. Consumer preferences are irrelevant as the business cannot conduct transactions without some personal information. Once it obtains this information, it must manage the risks created by use and disclosure. It can do this by identifying the personal information in its possession, and ensuring that appropriate policies are in force by auditing and generating reports on such uses and disclosures.

ENTERPRISE RISK MANAGEMENT

Enterprise risk management tools, said Blakely, are the best vehicle for protecting privacy. They complement lesser measures such as audit and access controls. These tools - technologies that help protect Internet privacy and the companies themselves – were also the subject of a presentation by Austin Hill, co-founder and Chief Strategy Officer of Zero-Knowledge Systems. He spoke of the company's new Enterprise Privacy Manager (EPM) software that allows organisations to define, implement and manage corporate privacy practices. This software could, for example, give different access rights and controls to various applications in an enterprise. The EPM will complement IBM's recently announced Enterprise Privacy Architecture.

SEPTEMBER 11TH

Although the conference was not intended as a forum on privacy issues flowing from the events of September 11th, such a discussion was inevitable. In a frank session on "trends and drivers" in privacy and business, Barry Steinhardt, Associate Director of the American Civil Liberties Union, argued that following September 11th, many companies attempting to sell government security equipment, were merely selling the illusion of security. Barbara Simons, of the Association for Computing Machinery, argued that security technologies are being used in the wrong way. For example, biometrics are being used to identify people, when they are best used for authentication.

Steinhardt added that the events of September 11th have led to an unholy alliance between business and government. Threats to privacy now come from both "Big Brother" and from industry, which is facing increasing pressure to act as the agent of the government.

Bob Belair, Editor of *Privacy & American Business*, argued that Americans have become less distrustful of government. This, he said, may lead to a significant, albeit temporary, changes in information relationships with government.

PRIVACY IN THE US – TWO PERCEPTIONS

Rick White, former US Congressman and founder of the Congressional Internet Caucus, argued that Congress will not pay attention to privacy issues in the present climate. Industry therefore has a chance to do a "better job" itself.

Philip J Bond, the US Under Secretary of Commerce, painted a different picture. He predicted, to the apparent surprise of many Americans in the audience, that omnibus privacy legislation would be introduced in Congress within a year. This legislation will deal with both online and offline privacy. The driving force behind this, he said, is the need to pre-empt a multiplicity of inconsistent laws, and the importance of building consumer confidence in dealings with the Internet.

Bond called the Internet the key to productivity, but acknowledged that there were serious concerns about the Internet environment. He spoke of the need to develop consumer confidence and trust, since e-commerce was a vital part of the economic future of the United States.

i

Zero-Knowledge Systems is making the conference CD-ROM available for purchase. It contains session proceedings, recap notes, presentations, speaker biographies, and photos in addition to enterprise and consumer product information and a copy of the company's Freedom Security and Privacy Suite 3.1. For further information visit: www.privacy.zeroknowledge.com/privacybydesign2001

New Zealand Comissioner criticises Complaints Review Tribunal

Privacy Commissioner, Bruce Slane, has attacked the Complaints Review Tribunal for painting over the cracks in its system by disposing of cases too quickly. The comments come after a year in which nearly half of all complaints passed over to the tribunal failed to receive a hearing.

In his annual report to the House of Representatives, Slane revealed that over 95 per cent of complaints submitted to the Privacy Commissioner were settled without further need for action. It prompts the conclusion that the remaining complaints were probably serious enough to require a hearing. Of the individuals denied "their day in court", nearly all were without legal representation. In his report, Slane stated: "I do not consider that the tribunal, in dealing with civil litigation, should take an early view that a matter has no merit. Rather, it should proceed to hear cases unless there has been a successful request by a respondent for a matter to be struck out."

He went on to cite a case in which the High Court found that the tribunal had acted incorrectly when refusing damages to an individual who was denied access to their health records. It was described by the High Court as a "classic case of proceeding on a wrong principle."

Slane believes that too many tribunal members are unsuitable to judge on privacy matters. However, he hopes to solve the problem through the recommendation that future appointees to tribunal boards have relevant experience or expertise when judging privacy cases.

For the full annual report, contact the Privacy Commissioner's office at: Tel: +64 (09) 302 8680, E-mail: privacy@iprolink.co.nz