Privacy and Security Conference 2007
"Identity Management and Information Protection in the Digital World: Can We Meet the Challenge"
February 15-16, 2007

Panel Session Summaries

The main theme of Privacy and Security Conference 2007 is identity management and information protection in the digital world. The focus is the impact that current identity management and information protection standards and practices have on the privacy and security of information shared between governments, businesses, consumers and citizens.

There is a summary provided below for each panel session to assist (but not limit) moderators and panelists in focusing their presentations to highlight these key issues and areas of concern. We trust the summaries will provoke discussion and debate amongst you as subject matter experts and that your presentations and comments at the conference will provide delegates with significant food for thought.

The panel summaries will also provide the basis for the description of the panels in the conference booklet.

Session 3 Panels (Thursday, February 15, 2007)

- **Panel A: National & Global Cyber Security: What's Needed, How Quickly?**

  Use of the internet has exploded in the last few years and individuals, governments and corporations nationally and globally now use the web not just to communicate, but to conduct business and provide, receive or monitor services. This puts enormous import on the safe and secure operation of these primary business, public service and communications networks. What happens if there are focused cyber-terrorism attacks or massive critical infrastructure failures? This panel session will look at what information security measures must be in place now to ensure that "cyber business" and SCADA systems are secure, who is doing what to accomplish this, and what we new issues we may face in the future.

- **Panel B: Managing Digital Identity: Data, Trust & Control**

  One of the most important issues for corporations and governments for conducting business effectively online is ensuring that the identity of the persons they are dealing with is verifiable and reliable. What is the best way to ensure this? Can technology ensure identity? How much information must be exchanged? Who controls the information and what role does trust play? Can data privacy be maintained?

- **Panel C: WiFi Zones: Privacy and Security Minefields?**

  Not only are wireless technologies increasingly prevalent in our communities, but some major cities offer citizens actual "WiFi zones" -- high-speed wireless networks where electronic information can be broadly transmitted by users through the airwaves within set geographical parameters. Toronto Hydro Telecom (THT) is the provider of the new "One Zone" WiFi network in the city of Toronto. What are the privacy and security considerations for governments and businesses of setting up a WiFi zone? How does using wireless technologies in WiFi zones impact users' privacy and security needs or expectations? What standards and interoperability requirements are necessary?

Session 6 Panels (Thursday, February 15, 2007)

- **Panel A: Biometrics and RFID: Controversial Identity Cure-Alls**

  Everywhere you turn, biometrics and RFID technologies are increasingly touted as the solution to securing and ensuring the identities of people traveling, working, purchasing or engaging on a multitude of other communal or commercial activities. From airports to workplaces to bars, facial or thumbprint biometric identification or RFID tags and readers are appearing as the most reliable means of ascertaining or affirming an individual's right to access to a product, receive a privilege or enter a location. But how reliable are biometric and RFID technologies for secure identification and identity management systems? Can their security be cracked or evaded? And what are their implications for privacy?

- **Panel B: Challenges in User Authentication: Are We There Yet?**

  Authentication is the primary component of digital identity management. It is the process used by corporations, government and other organizations to verify the online identity of individuals and subsequently grant them access to products or services. Authentication protocols provide organizations with the means to ensure that users of their systems or services are truly who they say they are. What are the best methods of user authentication? Is two-factor more secure than three-factor? What other techniques or methodologies are evolving? Can authentication be a relatively simple process or are many levels and layers required to ensure information privacy and security?

- **Panel C: Data Retention and "Lawful Access": Policing, Prosecution and ISPs**

  Every time we perform a transaction online, transactional data is created that identifies who we are and when and where the transaction took place. This data can be very important for law enforcement officials investigating and prosecuting crimes. While a court order is normally required for police to seize recorded information belonging to an individual, governments around the world are now modernizing legislation to facilitate more streamlined rights of search and seizure by police, given the great advances in electronic technology and, as a result, e-crime. But how do modernized data retention policies and lawful access rules impact the security expectations and privacy interests of citizens? Who owns transactional data? How long should it be kept? What are the responsibilities and requirements for service providers?

Session 9 Panels (Friday, February 16, 2007)

- **Panel A: Identity at the Borders: Modern Rules of Show and Tell**

  Since the September 11 terrorist attacks on the United States, both Canada and the US have taken significant steps to increase security at their borders. Citizens traveling by air, land or sea in North America have had to contend with new rules and stronger requirements for proving their identity. Similarly, government agencies charged with transportation security have quickly had to implement increased border security technologies and practices. What are the crucial elements of border security as it relates to

standards of identification and identity management technologies and practices? Can biometric, RFID or other electronic technologies guarantee traveler identity? And how is the personal information gathered by these technologies measured and used?

- **Panel B: Information Assurance: A Corporate Imperative**

  Information assurance (IA) is the practice of managing the risk associated with corporate information assets. Whether it is the confidentiality, integrity, privacy or availability of data that is at stake, it is in the government's or private sector agency's best interest to ensure that the storage, processing, transfer and disposal of their data is unthreatened by accident or malice. What are the best ways to do this? What are the biggest threats? And what typically are an organization's biggest weak spots?

- **Panel C: The Pros and Cons of Data Mining: Using Predictive Analytics to Improve Business**

  Data mining is unarguably an effective tool in assembling useful, usable information and knowledge out of sometimes vastly disparate aggregate data. It is frequently used by business to track consumer purchases and preferences and by governments to ensure the quality control and cost effectiveness of their services to citizens. Data mining, however, can also allegedly invade consumer and citizen privacy by tying together strands of information about individuals in ways that negatively impact or discriminate against them. This raises the questions: should data mining be regulated? Are there best practices so that legitimate business interests can be served but individual privacy interests are preserved? What, if any, measures of control such as notice or consent, should consumers and citizens have?

Session 11 Panels (Friday, February 16, 2007)

- **Panel A: Drivers Licences: The New National Identity Card?**

  With the US government's passing of the Real ID Act in 2005, which require state governments to comply with new national standards for drivers licences by May 2008, some American and Canadian jurisdictions are introducing drivers licences with new biometric or other technological security and identity management capacities that collect personal information. The Real ID Act also requires states to share their databases of drivers licence information.

Critics argue that these new requirements make drivers licences de facto "national identity cards" that can be readily used to track the free movement of individuals within and between countries. Supporters of the law, however, point out that the 9/11 terrorists used fake drivers' licences to board the airplanes they then used to attack Americans. What biometric and other digital technologies are being employed on the new drivers licences and are these technologies effective in securing and managing identities? What challenges do they propose to the traditional privacy rights and expectations of citizens?

- **Panel B: Corporate Data Breaches: Best Practices in Battling Identity Theft**

  Identity theft has been cited in numerous public and corporate surveys as a central concern by many consumers, governments and private agencies when conducting business online. The main issue affecting consumers is the potential for financial crimes that exploit their credit worthiness or good name by the carrying out of loan, mortgage, credit card and services frauds. For private or public sector agencies, the central issues are the cost of fraudulent transactions and the damage to consumer confidence in the organization's capacity to conduct secure online business transactions. What are the best ways for corporations and governments to secure themselves and their clients against the fraudulent use of personal information? Is identity theft primarily an internal or external security issue and can increased use of security technologies prevent it?

- **Panel C: Digital Signatures: Are They Reliable?**

  Digital signatures use asymmetric key algorithms or public key infrastructure schemes to secure and ensure that communications or electronic documents exchanged between users are authentic and senders and recipients are who they say they are. Critics claim however, that the legal and practical reliability of digital signatures suffers where it is suspected that a particular cryptosystem might have been broken, the key copied, or the whole scheme evaded in the first place by other means of obtaining unique identifiers. Supporters argue that no better means of authentication for electronic documents currently exist and that legislatures worldwide are moving to create laws recognizing its reliability for legal purposes. Are digital signatures sufficiently reliable? In what circumstance and for what purposes? Are there other options?