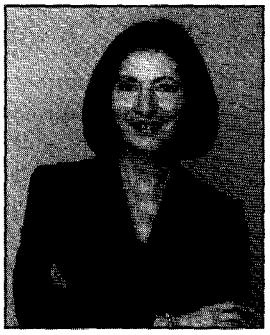
AN INTERVIEW WITH



Ann Cavoukian

Dr. Ann Cavoukian is recognized as one of the world's leading privacy experts. She oversees the operations of the freedom of information and privacy laws in Ontario, Canada, in her role as Information and Privacy Commissioner (IPC). Dr. Cavoukian joined the Office of the IPC as its first Director of Compliance in 1987. Prior to joining the IPC, she headed the Research Services Branch for the provincial Attorney General. She received her M.A. and Ph.D. in Psychology from the University of Toronto, where she specialized in criminology and law, and lectured on psychology and the criminal justice system.

Her published works include *Who Knows: Safeguarding Your Privacy in a Networked World,* with Don Tapscott (McGraw-Hill, 1997), and *The Privacy Payoff: How Successful Businesses Build Consumer Trust,* with Tyler Hamilton (McGraw-Hill Ryerson, 2002).

What is information privacy?

Information privacy essentially revolves around personal control—an individual's right to control the collection, use, and disclosure of his or her personal information. Freedom of choice is vital. Personal information is information that relates to an "identifiable individual." Organizations that collect, use, and disclose personal information can protect an individual's right to privacy by implementing what are commonly referred to as "fair information practices." Fair information practices are a set of common standards that balance an individual's right to privacy with the organization's legitimate need to collect, use, and disclose personal information. In Canada, fair information practices are set out in the *Canadian Standards Association Model Code for the Protection of Personal Information* (the CSA Code). At the international level, I chaired a working group of data protection and privacy commissioners convened for the purpose of creating a single Global Privacy Standard (GPS), which was formally tabled and accepted by Commissioners in 2006 at the 28th International Data Protection Commissioners Conference in the United Kingdom.

The CSA Code consists of ten principles. First, it requires the designation of at least one individual who is accountable for the organization's compliance with the other nine principles (**Accountability**). The organization must specify the purposes for which it collects personal information, at or before the time when the information is collected (**Identifying Purposes**). The consent of the individual must be obtained for the collection, use, or disclosure of personal information, except where it is not appropriate to obtain consent (**Consent**). The collection of personal information must be limited to that which is necessary to fulfill the specified purposes (**Limiting Collection**). Personal information must not be used or disclosed for purposes other than those for which it was collected, unless the individual consents or as required by law (**Limiting Use, Disclosure,** and **Retention**). Personal information must be as accurate, complete, and up-to-date as necessary for the purposes for which it is to be used (**Accuracy**). The organization must implement security safeguards that are appropriate for the level of sensitivity of the personal information (**Safeguards**). The organization must make readily available specific information about its policies and practices relating to the management of personal information (**Openness**). Individuals have a right to access and request correction of their own personal information (**Individual Access**). Finally, individuals must be able to challenge an organization's compliance with the privacy principles (**Challenging Compliance**).

The GPS is based on the same underlying principles as the *CSA Code:* Consent; Accountability; Purpose; Collection Limitation; Use, Retention, and Disclosure Limitation; Accuracy; Security; Openness; Access; and Compliance. However, with respect to the principle that the collection of personal information should be limited to that which is necessary for the specified purposes, the GPS goes further by emphasizing the need for data minimization. Data minimization requires the collection of personal information to be kept to a strict minimum. This means that the design of programs, information technologies and systems should begin with nonidentifiable interactions and transactions as the default. Wherever possible, the identifiability, observability and linkability of personal information should be minimized. Also, in terms of accountability the GPS goes further than the *CSA Code* by requiring the documentation and communication of privacy policies and procedures, as well as the designation of a responsible person, and by requiring organizations to seek equivalent privacy protection through contractual and other means when transferring personal information to third parties.

People often sacrifice information privacy for the sake of convenience. Is information privacy really important?

Consumers are sometimes willing to provide personal information in exchange for some benefit or service. For example, consumers are sometimes willing to register personal information on a Web site in exchange for useful information or a discount on merchandise. It is up to each individual consumer to weigh the cost and benefits of providing personal information in any given situation—it's his or her choice. As long as this collection of personal information takes place with the knowledge and consent of the individual, it is not an invasion of privacy—it is a matter of personal choice and control which is central to the concept of privacy. When information is collected, used or disclosed without the knowledge or consent of the individual, then privacy becomes an issue.

How has 9/11 affected people's attitudes toward information privacy?

Immediately after 9/11, people seemed willing to sacrifice civil liberties and privacy if necessary, in order to feel secure. There was a surge of support, particularly in the United States, for increasingly invasive security measures and expanding public surveillance. However, as time passed, heads cooled and the public began to think more rationally about these issues and whether or not the invasive security measures that were being implemented and contemplated would actually having the desired impact on national security. The public began to question whether the privacy sacrifice that we were all being asked to make was actually worth it. In June of 2007, federal, provincial and territorial privacy commissioners across Canada united in calling for the federal government to suspend its new no-fly list program until it could be overhauled to ensure strong privacy protections. The Passenger Protect Program involves the secretive use of personal information in a way that will profoundly impact privacy and other related human rights, without legally enforceable rights of appeal to independent adjudication or to compensation for expenses and damages.

The public's interest in protecting consumer privacy, however, did not diminish in the post-9/11 period. If anything, the value of trusted business relationships has increased.

Information about customers is a valuable commodity. Why should a business be concerned about protecting the privacy of its customers?

In Canada, it happens to be the law for private sector organizations, but a simple answer to the above question is that, "privacy is good for business!" This assertion is supported by a Harris/Westin Poll where in November 2001 and February 2002, it was found that if consumers had confidence in a company's privacy practices, they were much more likely to increase volume of business and frequency

of business with that company. Conversely, they were likely to stop doing business with a company if it misused personal information. Further, The Information Security Forum reported in 2004 that a company's privacy breaches can cause major damage to brand and reputation. Robust privacy policies and staff training were viewed as keys to avoiding privacy problems.

Organizations that do business in the U.S. may be subject to one or more recently enacted breach notification laws that require organizations to tell consumers when their personal information has been breached. These laws have helped to expose numerous serious privacy breaches. Such breaches can have serious consequences for both the individuals whose privacy is breached and the organization that is responsible for the breach. For example, the *Wall Street Journal* reported in May 2007 that following the TJ Maxx breach, involving the theft of 45.7 million credit and debit card numbers, banks could be forced to spend $300 million to replace cards and that the breach could result in $20 million in fraudulent transactions. The potential costs and harm to an organization's reputation provides a further incentive for organizations to think proactively to prevent privacy breaches.

Do you favour opt-in policies over opt-out policies?

As a general rule, opt-in policies are viewed as being more privacy-protective than opt-out policies. However, the type of consent that an organization should obtain (i.e., opt-in versus opt-out) depends on the circumstances in which personal information is being collected, used and disclosed. When it is reasonable in the circumstances to infer implied consent, an opt-out type of consent may be appropriate, particularly where the information is not considered to be sensitive. For example, the individual's name and address may not be considered to be sensitive, and the collection of this information for specified purposes may take place with an opt-out type of consent. On the other hand, opt-in consent should generally be obtained whenever sensitive personal information, such as medical information or financial information, is being collected, used or disclosed.

Is Canada ahead of the United States with respect to ensuring fair information practices?

Canada has more comprehensive privacy and data protection laws and statutory oversight/enforcement agencies. By contrast, the U.S. has a multitude of specialized, sectoral laws, regulations and self-regulation and more scope for private rights of action and financial penalties. There is strong evidence that Canadian organizations are more aware of privacy and much more likely to apply privacy principles throughout their operations than U.S. firms.

For example, in a benchmark study conducted by my office and the Ponemon Institute—a Tucson, Arizona–based "think tank" dedicated to the advancement of responsible information management practices within business and government—we compared the corporate privacy practices of Canadian and U.S. businesses. Some of the key findings of the study were that in comparison to U.S. companies, Canadian companies:

- are more likely to have a dedicated privacy officer and a privacy program with a clearly articulated mission,
- are more likely to have a formal redress process for customers to respond to queries and concerns about privacy,
- are more open to providing customers with the right to access and correct personal information,
- offer more choice to customers and consumers in terms of opting out (or opting in) to secondary uses and disclosures of personal information,
- are less likely to sell customer data,
- are more likely to offer privacy training or awareness programs for employees and contractors who handle sensitive personal information,

- hold their vendors and other third parties to higher standards or due diligence requirements,
- have a more aggressive data control orientation when collecting and retaining sensitive personal information,
- are more concerned about insider misuse than external penetration,
- require more rigorous data quality controls and monitoring requirements for transacting and moving of personal information about employees and customers, especially when the application involves transborder movement, and
- are more likely to have strict policies that protect the privacy of employees.

As you ponder new threats to information privacy, are there any emerging technologies you find particularly troubling?

A qualified answer would include item-level Radio Frequency Identification (RFID) tags; conventional biometric and other forms of authentication and identification; data mining; and video surveillance. If these emerging technologies are designed and implemented with fair information practices in mind, then they can enhance and enrich our lives immeasurably. But if used surreptitiously and without regard for privacy, they only hold the promise of an untenable scenario of ever-present surveillance and discrimination, the proverbial "Orwellian nightmare." It all depends on the design and configuration of a particular technology.

It is also important to note that there are emerging technologies that can actually help us to protect our privacy. Such technologies are generally referred to as Privacy Enhancing Technologies (PETs). For example, Biometric Encryption is a PET that allows you to use your biometric to encrypt a PIN, a password, or an alphanumeric string, for numerous applications—to gain access to computers, to enter buildings, and to privately and securely prove identity, etc. This represents an enormous gain to privacy and heralds the growth of a new area of privacy-enhancing biometrics under the emerging category of untraceable biometrics.