Information and Privacy
Commissioner of Ontario
Commissaire à l'information
et à la protection de la vie privée de l'Ontario

Commissioner issues challenge to technologists: Take the next STEP

By Ann Cavoukian, Ph.D.
Information and Privacy Commissioner of Ontario

January 10, 2002

Today, I am issuing a challenge - a privacy challenge, asking you to take the next step. My office recently launched a new initiative called STEPs, short for Security Technologies Enhancing Privacy, that will hopefully revolutionize the traditional way in which privacy and security are viewed.

There has always been a natural tension between security and by this I mean public safety and privacy. However, the fine balance that has traditionally been struck in our open, democratic society recently suffered a severe blow, a double blow in fact. First, the terrorist attacks of Sept. 11, 2001 (and subsequent anthrax scares) shocked us out of our collective sense of comfort and safety. Second, the reaction, or over-reaction, of governments (in Canada, the United States, the United Kingdom and elsewhere) struck privacy a heavy blow when the balance between civil liberties and public safety was redrawn.

Yes, it is true that extraordinary times (such as those we are facing today) call for extraordinary measures, but one must question whether such times will extend without limit into the future, and whether all the newly invoked measures in Bill-36, the *Anti-terrorism Act*, and other public safety legislation are truly warranted and necessary, without, in most cases, an end in sight to their application.

Security and Privacy

Even in the face of increased levels of police surveillance and detection measures, however, there are new ways that we can promote the protection of privacy. I am advancing the view that the very same technologies now being used to help fight terrorism can also be used to enhance privacy. While this may seem counter-intuitive at first, I believe that not only can such a view be made to work, but that it must be made in order to preserve our sense of dignity and personal autonomy - the future of privacy may well depend on it.

Let me explain: The essence of the problem revolves around the traditional model of viewing privacy and security as polar opposites. Security and privacy have always been viewed as opposing forces in a zero-sum game paradigm. Such a view, by necessity, invokes a balancing act because, in a zero-sum game, the more you have of one, the less you can have of the other. This win-lose approach does not bode well for privacy. The greater the steps taken for public safety and security, the greater the erosion of our privacy.

This is why we must change the paradigm to a win/win model. There is no inherent reason why a zero-sum approach must be taken. Once we reframe our mindset from believing that we must cede privacy in order to have security, then we can take the necessary steps to improve security while minimizing the privacy invasiveness of many technologies.

If we substitute the view that privacy and security are complementary to be regarded as two sides of an indivisible whole, then we can design ways to protect public safety without sacrificing our privacy in the process. However, the more we are willing to compromise just a "little bit" of privacy in the name of security, the greater the likelihood that over time, we will ultimately compromise most if not all of our privacy.

STEPs

A number of technologies have been promoted over that last few years that I would describe as "Privacy-Enhancing Technologies" (PETs, a term that my office coined in 1995), which minimize the use of personally identifying information, through encryption software, anonymizers, pseudonomizers, and "cookie-cutter" programs for Web browsing. I believe that it is now time to take the next step - to take the PETs message to the mainstream security market. In doing so, I am suggesting that potentially privacy invasive technologies, such as biometrics, electronic surveillance, data mining, and various types of imaging, sensing and other emerging technologies, can be reframed and designed to serve as effective security tools in the fight against terrorism, yet not give away privacy in the process.

Shifting to a new paradigm in the security/privacy context is not as far-reaching as some may think, but it will clearly involve creative, innovative "thinking out of the box." To this end, I am issuing a challenge to all vendors and technologists presently offering "security solutions" to step up to the privacy bar. I firmly believe that privacy can be built into the design of most security technologies, enabling them to take the next step - becoming Security Technologies Enhancing Privacy, or STEPs.

By building privacy safeguards into the design and framework of security technologies, we can both improve the actual safety of our airports, offices and computer networks, without creating the tools and conditions that allow for unchecked data mining, massive surveillance and invasive body scanning. Equally important will be development of sound policies incorporating security/privacy-related technologies into the standard operating procedures and practices of organizations.

I acknowledge that this task will not be easy, but consider the alternative. In my view, it would be the ultimate irony if we had to give up our rights and freedoms in our effort to secure them. By changing the security/privacy mindset from a zero-sum game to one that frames security around a "privacy by solution" concept, we will significantly move the yardstick towards more privacy-protective solutions to our security-related concerns. I ask that you take the next STEP in favour of both privacy and security.