Information
and Privacy
Commissioner/
Ontario

Security Technologies Enabling Privacy (STEPs):

Time for a Paradigm Shift

Ann Cavoukian, Ph.D.
Commissioner
June 2002

Information and Privacy
Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

This publication is also available on the IPC website.

Table of Contents

The Context

The death and destruction wreaked by the terrorist attacks of September 11, 2001 had a profound impact on individuals and governments around the world. In North America, the Canadian and United States governments immediately made public safety and security their highest priority, quickly passing sweeping anti-terrorism legislation that dramatically expands police and surveillance powers. New controls on physical movement and identity verification were imposed at border control points and airports.

In this climate of crisis, government respect for principles of privacy has suffered a major setback. Government officials acknowledge that privacy is important, but insist that in light of the scale of carnage on September 11, ensuring the public's safety and security has become paramount. New institutional controls are essential, and if they come at the expense of civil liberties, so be it; the benefits outweigh the cost. So far, much of the public seems to accept this reasoning, though support for some of the more extreme safety and security measures proposed, such as identity cards,[1] now seems to be slipping.

Historically, privacy and security have been treated as opposing forces in a zero-sum game. Such a view, by necessity, invokes a balancing act, where the greater the gains for ones side, the greater the losses for the other. In a game theory paradigm, the more you have of one, the less you can have of the other, so that the sum always remains "zero." But this win/lose attitude poses a major threat for privacy, since the public's desire for safety and security is so high. Continuing the post 9/11 debate within this framework threatens the very foundation of privacy, leaving its future in question.

This is why we must change the paradigm. This paper argues there is no inherent reason why greater safety and security must come at the expense of privacy. If we can reframe the issue, challenging the underlying premise that we must cede privacy in order to gain security, then we can take the necessary steps to improve both. Many security technologies can be redesigned to remain highly effective, while at the same time, minimizing or eliminating their privacy invasive features. If we substitute a new premise - that privacy and security are two complementary sides of an indivisible whole (not polar opposites), then we can design technologies that protect public safety without sacrificing privacy.

[1] On 12 March 2002, Gartner announced the results of its survey on establishing a U.S. national identity database. The survey found:

- 41 percent of U.S. citizens oppose creating a national ID database to identify citizens and visitors to the United States.
- Only 26 percent of U.S. citizens agreed to such a database.
- Opposition to a national ID database ran particularly strong in the southern, western and midwestern regions of the United States.
- U.S. citizens ranked private institutions — especially banks and credit card companies — as more trusted than government agencies to administer a national ID program.
- Among government agencies, the U.S. Federal Bureau of Investigation ranked as the most trusted to manage a national ID database, followed closely by the Social Security Administration. Least trusted were state motor vehicle departments and the Internal Revenue Service.

Shifting to a new paradigm that incorporates both privacy *and* security is not as difficult as it may seem. Take, for example, the passenger scanning technologies deployed at airports. Body scanners display everything under a person's clothing, including concealed weapons, chemicals, restricted objects and the body itself. But there is no security need for the equipment operators to view the essentially "naked" bodies of passengers. Equally effective but much less privacy-invasive technology exists. 3-D holographic imaging using millimeter-wave scanning techniques also reveals any hidden objects but not the subject's body image itself – security *and* privacy in one technology. Not only is this a desirable goal, it is a feasible one. Technologies are slowly beginning to emerge that incorporate both features in their design.

The Challenge

We need to champion the creation and use of security technologies that enable privacy, such as the holographic imaging scanner noted above. For this, we believe that a three-pronged strategy is required.

The first component rests with privacy commissioners and privacy advocates. It is our challenge to raise the level of debate on security and privacy above traditional, simplistic, either/or viewpoints. This begins by examining the democratic underpinnings and values that need to inform our actions, and by questioning the paradigm assumptions that pit security against privacy. There is an important role for the privacy community to play in championing privacy in technology, public policy and legislation.

A second component rests with a group I will describe as “specification writers.” This encompasses two groups: 1) legislators, policy analysts and legal counsel that draft legislation focused on security and public safety, and 2) directors, managers, individuals, who develop Requests for Proposals (RFPs) and set the ‘specs’ for the contractors and consultants being procured to provide security technologies.

On the legislative side, elected officials and their staff could begin by reviewing the legislation passed so hastily after September 11. If it can be shown that amendments are appropriate, then legislators should adopt them. An example of this type of review concerns the various exemptions to Canadian federal privacy legislation that *The Anti-Terrorism Act* introduced. (On a promising note, Bill C-42 – the *Public Safety Act*, which had received first reading, was subsequently abandoned for being too far-reaching.) We need to develop creative solutions to ensure that the legislation provides for independent oversight, such as that formerly provided by the Privacy Commissioner of Canada. We need accountability and a form of transparency, achieved in ways that do not diminish public safety or hamper intelligence-gathering and law enforcement. For example, independent oversight by a judicial committee, or an inter-party committee of the legislature, can provide additional privacy safeguards.

As for the specification writers developing RFPs and setting out contracts for security vendors, an education and orientation process could dispel a number of privacy misconceptions on their part. Experience has shown, for example, that privacy is often mistaken for such things as access controls, authentication mechanisms, and data quality – all security-related issues. While security is an important component of privacy, it is only one ingredient. The term “privacy” subsumes a much broader spectrum of protections that extend beyond security alone. Thus, the two terms cannot be used interchangeably, although this is a common misconception.

Education is a key mandate of the Information and Privacy Commissioner of Ontario (IPC) — a role shared by privacy and data protection commissioners around the world. These organizations are keen to help bring the values, and perhaps more important, the vocabulary of privacy, to the 'security table.' Motivated spec writers can begin by reading documents dealing with these issues on Commissioner Web sites,[2] or engaging their respective Commissioners through meetings or project participation.

The third component of the strategy lays with the 'solution providers' - the developers of technology and their industry associations. These companies, whether involved in the development of biometrics, smart cards, scanning technologies, registration systems, or database design and management, need to introduce privacy concepts into the policy statements of their organizations and associations. Privacy must be incorporated into the concept, design and implementation of their technology solutions. A number of companies have already demonstrated that privacy can be an effective strategic opportunity.[3]

Security technology companies may be in a difficult position regarding privacy when servicing government or private sector contracts. While popular thinking suggests that 'privacy has taken a big hit' in the government/public safety space, this sentiment should not be misunderstood as extending to the business community. Privacy expectations for the private sector continue to climb - it's business as usual. As noted earlier, the public's appetite for security systems such as national ID cards has already started to wane.[4] It is in a company's best interests to stay ahead of the privacy curve, since the cost of mistakes can be very high.[5] At the very least, an organization should conduct a privacy-threat risk assessment before designing or developing a security technology. If a technology does in fact threaten privacy, the organization should invest the intellectual capital and time to build in privacy protections. Case studies have shown that the additional cost of this work is negligible, at this time, often only one per cent of the full implementation of a technology solution.[6]

Some companies are starting to incorporate privacy principles into the design and deployment of their technologies. This ethical commitment ensures that security and privacy are paired as partners in the fight against terrorism. In the United States, the White House has indicated its commitment

[2] For a starting place go to www.ipc.on.ca and go to links to other jurisdictions.

[3] The Royal Bank of Canada has seen the value of privacy as strategic opportunity. See American Banker, February 20, 2002.

[4] "Support for ID cards waning," Wired News. www.wired.com/news/business/0,1367,51000,00.html, 13/03/02.

[5] Some examples of negative public reaction: "Guess.com leaks credit card numbers of the fashion conscious," www.theregister.co.uk/content/6/24315.html. "Comcast continues to snoop," www.mlive.com/news/aanews/index.ssf?/xml/story.ssf/html_standard.xsl?/base/news/1013845208161454.xml. "Netscape Navigator browser snoops on web searches," www.newsbytes.com/news/02/175035.html.

[6] "Guaranteeing requirements of data-protection legislation in a hospital information system with privacy-enhancing technology," The British Journal of Healthcare Computing & Information Management, 04/98 Vol. 15 n. 4, p. 31.

to protecting privacy when assessing security technologies used in the fight against terrorism. John Marburger, Science Advisor to the U.S. President, said, “The president is very committed to not undermining the civil liberties we are fighting to preserve.”[7]

Industry associations also have a key role to play in setting out privacy principles and helping their members become privacy literate. The International Biometric Industry Association (IBIA), for example, has mapped out a set of privacy principles for its members. It is in the process of hiring a chief privacy officer and is seeking advice from privacy experts, including IPC staff. Together with the Canadian Advanced Technology Alliance (CATA) Biometric group, the IBIA has offered to partner with the IPC to ensure that security technologies incorporate privacy protections. One of the first steps will be to develop a set of privacy design specifications that can be used by both technology developers and those who purchase the technology. Before that, however, it is important to understand the current landscape regarding security technologies and take stock of the extent to which privacy is addressed. We must also examine the potential to introduce privacy enabling characteristics into security technologies that are in various stages of development or design.

[7] “On the ultimate questions that might have an impact on civil liberties, the president himself is going to have to weigh in,” Marburger said. *White House Stressing Civil Liberties in Homeland Security Plans*, washingtonpost.com, May 29, 2002, www.washingtonpost.com/wp-dyn/articles/A29017-2002May29.html.

An Overview of Security Technologies and their Privacy-Enabling Characteristics

Technologies can be grouped according to their purpose, and examples of the specifics of each category are given below. Some technologies may belong to more than one group.

Surveillance Any technology aimed at tactically observing an activity to thwart illegal or harmful behaviour, or recording and documenting its occurrence. Typical technologies would be Closed Circuit Television (CCTV), digital and optical video.

Identification Any technology aimed at positively identifying an individual. Typical technologies include identification pass cards (magnetic strips), and biometrics (e.g., fingerprints, retinal scans, etc.).

Threat Prevention Any technology aimed at detecting specific threats to people or property. Typical technologies include bomb detection scanners at airports and thermal imaging scanners.

Tracking and Monitoring Any technology aimed at ongoing recording of the trail or activities of specific individuals or profiled groups. Typical technologies include taping and recording of telephone conversations, interception of e-mail, and online recording, tracking and monitoring of travel patterns.

Intelligence Systems Any technology aimed at collecting, organizing, sorting, analyzing and assessing criminal, intelligence and investigative data.

STEPs Opportunities and Examples

The following are several examples of STEPs technologies and instances where privacy specifications have or could be introduced into security technology development.

STEP Example: 3-D Holographic Body Scanner

Passenger scanning technologies are commonplace at all airports and are deployed to identify possible security threats. However, scanning technology has the potential to intrude on the physical privacy of the individuals being scanned. Researchers at the U.S. Department of Energy have developed a new technology that augments security scanning while addressing this privacy concern.

The Department's Pacific Northwest National Laboratory have produced a scanning technology, using 3-D holographic imaging, that focuses on revealing objects hidden underneath the clothing of airline passengers, instead of displaying the entire body. In addition to metal weapons, those made of plastic and ceramics can be detected by the Personal Security Scanner, thus offering a distinct advantage over surveillance systems that rely on metal detectors alone. The scanner uses non-harmful ultrahigh-frequency radio waves with relatively large wavelengths that can penetrate clothing. Concerns that the unclothed physical features of a person being scanned might be visible to the scanner operator were addressed by reprogramming the system to give the operator a view of only concealed items, and not the person's image. The Personal Security Scanner is an excellent example of technology that is designed and deployed in a manner that addresses security requirements while minimizing the intrusion into personal privacy.

STEP Example: Biometric Encryption

Biometric encryption is an ideal example of a security technology that enables privacy because privacy is built into the very design of this technology. A person's biometric, such as a fingerprint, is used as part of the encryption algorithm to uniquely encrypt a PIN number or any alphanumeric. One's biometric serves much like a private encryption key. All the security features of a biometric are preserved – only the individual with a particular biometric can gain access to an account or computer system, or enter a building. But the biometric could never be used to serve as a universal identifier. The reason for this is quite simple: Since one's biometric is used to encrypt a different number or alphanumeric for each application, there is no *single* template of a biometric generated that remains. Therefore, it is not possible to link (for tracking or profiling purposes), the trail of biometrics left behind because there is no single biometric whose footprints you would track – each one is unique, thereby being incapable of being linked or matched. Biometric encryption defies data linkage at a systems level, thereby offering the greatest protection of privacy. The individual maintains complete control.

STEP Opportunity: Project Oxygen

"Project Oxygen" is an organization of 30 faculty members from MIT's Laboratory for Computer Science (LCS). The lab's mission statement is "Going after the best, most exciting forefront technology; and ensuring that it truly serves human needs." While pursuing ventures that are "research aimed at replacing the PC with ubiquitous, often invisible computing machines," they are also employing principles similar to those underlying STEPs. Victor Zue, of the LCS states, "Privacy is one of four interlocking issues that we must address in a pervasive, human-centered world."

STEP Opportunity: Canadian Air Transport Security Authority

The Canadian Air Transport Security Authority (CATSA) was established in December 2001 to enhance pre-board screening. Its mandate includes establishment of consistent pre-boarding reviews of passengers, advanced explosion detection equipment and expanded policing at airports and aboard aircraft. Since the authority will be responsible for 99 per cent of all passenger air traffic, it would be an excellent place to introduce privacy specifications into the design, development and implementation of security technologies. Since CATSA is relatively new, officials are still considering its mandate.

Airport authorities were initially skeptical that security technologies that could actually be deployed with privacy specifications. This is not particularly surprising since their job is to protect airports and the traveling public, not privacy. However, the federal Treasury Board approved a new Privacy Impact Assessment policy, to come into force in May 2002, which **requires** agencies such as the CATSA to carry out detailed Privacy Impact Assessments on any new or changing initiatives involving personal data.

To advance the STEPs concept, the IPC is partnering with the Greater Toronto Airport Authority to develop best privacy practices for security technologies that are being planned for implementation. These technologies include: identification systems, automated flight registration (check-in) systems, voluntary frequent traveler systems, and physical access security screening systems. The focus of these best practices will be on the data collection and processing rules and protocols, with a mind to minimizing their potential for unwarranted privacy invasions.

STEP Opportunity: Transportation Security Administration

The U.S. Department of Transportation houses the newly formed Transportation Security Administration (TSA).[8] The TSA's goal is to continuously set the standard for excellence in transportation security through its people, processes, and technologies. One paper they released surveys aviation security technologies and gives recommendations on which are the most promising.

The TSA selected Boston's Logan International airport to test various security tools. We believe Logan would be an excellent testing ground for STEPs. State Police at the airport use wireless hand-held PCs for random checks on crew, staff and travelers. The devices connect to the National Crime Information Center, allowing police to check criminal information instantly, including outstanding warrants, stolen car information and criminal histories. The airport is also testing new document authentication technology to detect false passports or IDs.

[8] Transportation Security Administration, www.tsa.dot.gov/.

STEP Opportunity: Biometric Consortium

The Biometric Consortium is the U.S. Government's focal point for research, development, testing, evaluation, and application of biometric-based personal identification/verification technology. That site lists a large number of biometric initiatives, many of which are potential future STEPs. There is no indication at this point that the Consortium is actively considering privacy standards in any of its development.

STEP Opportunity: Super Bowl Biometrics

John D. Woodward, author of "Super Bowl Biometrics," identifies the requirements that must be met before the government could use a biometric database identification system to identify suspected criminals or terrorists. These requirements could be used to develop a Security Technology Privacy Test, to ensure that such technologies fulfilled their intended purpose and met privacy specifications. The requirements include making the government entity demonstrate how the collection of personal information is required; reveal how and where the data will be stored; how, when and with whom it might be shared; require the routine purging of the database to ensure that data is current and accurate, and introduce strict safeguards to ensure the data is not disclosed without authority. The government would also need to make all of the above publicly available. In addition, Woodward suggests that there be some sort of oversight for the database. In essence, he follows the script of fair information practices, describing most of the ten principles in Canada's *Personal Information Protection and Electronic Documents Act*.

STEP Opportunity: Deployment at Thunder Bay International Airport Authority

The Thunder Bay International Airport Authority (TBIAA) is using the NEXUS Group Internationals' AcSys Biometrics Corp. face recognition system. Conquest Alliance Group Inc. in Burlington, Ontario, is teaming with CompuBlox Inc., another Canadian firm, to pilot the technology through a Transport Canada project. The system employs a smart card that is verified with a facial scan. The TBIAA has as its mission, "to realize superior standards of customer service ... focusing on growth, safety and efficiency." While the pilot project is restricted to authorized personnel, the partners in the project appear to be testing solutions for larger-scale implementation.

STEP Opportunity: Non-Governmental Organizations/Associations

The International Air Transport Association (IATA) has created an Airport Security Working Group.

Airport security involves many actors. Airport authorities are looking for processes and technologies to enhance security. The U.S. Transportation Security Administration is looking for security standards nation-wide (as is the Canadian Air Transport Authority in Canada), while the technology sector, which has been working on such tools and marketing them to a "mild" market before September 11, now appear to be the source for the solutions these entities are seeking. The airlines say they are doing the best they can with their existing tools, re-arranging processes and physical security issues where possible. But they are not in the business of bio-identity or passenger profiling, unless they find it a positive customer issue or need to do so in order to accommodate government requirements imposed upon them.

Associations like IATA and the American Air Transportation Association parallel the efforts of the TSA and the Canadian Air Transport Authority. The IPC will be approaching the IATA to highlight privacy concerns as it develops various security and secure travel initiates. Numerous other international aviation organizations such as the International Civil Aviation Organization may also be approached to include a discussion of privacy in their security programs.

Cost Considerations

Part of the challenge of introducing privacy enabling specifications into security technologies is addressing the increased cost. It is easy for skeptics to claim that adding privacy requirements to the mix will increase existing costs dramatically. While some additional costs will no doubt be entailed, we need informed cost projections for STEPs products and systems, not unrealistic conjecture. Organizations must also consider the cost implications of not implementing privacy provisions into their security systems – potential prosecution for violation of legislation, civil litigation, adverse publicity, etc.

Even without considering special privacy features, the cost of security technologies can vary widely; for example, the cost of devices used by airports to scan and examine passenger luggage. A computerized tomography (CT) device, which is based on advances made in the medical field, offers the best overall detection ability but is relatively slow in processing luggage and has the highest price, at approximately $1 million (all funds in U.S. dollars) each. The Federal Aviation Administration (FAA) certified this device in December 1994. On the other hand, two advanced X-ray devices are available that have lower detection capability but are faster and cheaper, costing approximately $350,000 to $400,000 each.

At least five manufacturers sell devices that can detect the residue or vapour from explosives on the exterior of carry-on bags and on electronic items, such as computers or radios. These devices, also known as "sniffers," are commonly referred to as "trace" detectors and range in price from about $45,000 to $170,000 each. Two other devices, based on electromagnetic technology, are in development. Rather than detecting particles or vapour, these devices will provide images of items concealed under passengers' clothing. Prices are expected to be approximately $100,000 to $200,000. The FAA and the Department of Defense are developing devices that passengers may find more acceptable. FAA estimates that it would cost $1.9 billion to provide 3,000 of these devices to screen passengers.

These examples demonstrate that security technology encompasses a broad spectrum of costs and capabilities. The cost of ensuring that these technologies also address privacy issues needs to be realistically assessed. As indicated in the "Examples and Opportunities" section, these costs are not necessarily either significant or prohibitive.

Conclusion

As we have outlined above, the STEPs approach is clearly in its infancy. While there are at present few security technologies and technology development companies that demonstrate an understanding that privacy and security safeguards can co-exist (as reflected in their products), much more needs to be done – this work has only just begun. The Information and Privacy Commissioner of Ontario, in posing the challenge presented in this paper, is offering a new paradigm for viewing the relationship between security and privacy – one of interdependence, not opposing forces. We must abandon the zero sum paradigm. We call upon specification writers, solution providers, software designers, and technology developers to step up to the challenge. A paradigm shift of the magnitude we are seeking will take a great deal of effort, and more importantly, a great deal of will, before its adoption can become widespread. Only then can privacy and security co-exist, with an understanding that both are essential ingredients in preserving a world where our freedoms will prevail. That is our vision – that is our goal.

Information and Privacy
Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca