Information and Privacy
Commissioner of Ontario

Transformative Technologies Deliver Both Security and Privacy: Think Positive-Sum not Zero-Sum

Ann Cavoukian, Ph.D.

Information & Privacy Commissioner
Ontario, Canada

Privacy, in the form of informational privacy, refers to an individual's ability to exercise personal control over the collection, use and disclosure of one's recorded information. Thus far, a "zero-sum" approach has prevailed over the relationship between surveillance technologies and privacy. A zero-sum paradigm describes a concept or situation in which one party's gains are balanced by another party's losses – win/lose. In a zero-sum paradigm, enhancing surveillance and security would necessarily come at the expense of privacy; conversely, adding user privacy controls would be viewed as detracting from system performance. I am deeply opposed to this viewpoint – that privacy must be viewed as an obstacle to achieving other technical objectives. Similarly, it is unacceptable for the privacy community to reject all forms of technology possessing any surveillance capacity and overlook their growing applications.

Rather than adopting a zero-sum approach, I believe that a "positive-sum" paradigm is both desirable and achievable, whereby adding privacy measures to surveillance systems need not weaken security or functionality but rather, could in fact enhance the overall design. A positive-sum (win-win) paradigm describes a situation in which participants may all gain or lose together, depending on the choices made.

To achieve a positive-sum model, privacy must be proactively built into the system (I have called this "privacy by design"), so that privacy protections are engineered directly into the technology, right from the outset. The effect is to minimize the unnecessary collection and uses of personal data by the system, strengthen data security, and empower individuals to exercise greater control over their own information. The result would be a technology that achieves strong security *and* privacy, with a "win-win" outcome.

By adopting a positive-sum paradigm and applying a privacy-enhancing technology to a surveillance technology, you develop, what I am now calling, "transformative technologies." Among other things, transformative technologies can literally transform technologies normally associated with surveillance into ones that are no longer privacy-invasive, serving to minimize the unnecessary collection, use and disclosure of personal data, and to promote public confidence and trust in data governance structures.

Positive-Sum Paradigm + Privacy-Enhancing Technology
(Applied to Surveillance Technology) = Transformative Technology

Surveillance Technologies

Whether real-time or offline, we are all increasingly under surveillance as we go about our daily lives. Surveillance control technologies generally include (typical objectives):

- Public and private video surveillance (public safety)
- Employee monitoring and surveillance (corporate data security)
- Network monitoring, profiling and database analytics (network forensics, marketing)
- Device location tracking (safety, resource allocation, marketing)
- "Whole of customer" transaction aggregation (customer service)
- Creation and uses of "enriched" profiles to identify, verify and evaluate (security)
- Creation and uses of interoperable biometric databases (access control/security)

Like hidden one-way mirrors, surveillance reflects and reinforces power asymmetries that are prone to misuse. By monitoring and tracking individuals, surveillors can learn many new things about them and use that knowledge to their own advantage, potentially making discriminatory decisions affecting the individual.

The objectives of monitoring and surveillance, however, may be quite justifiable and beneficial. The basic proposition of many surveillance systems is that usersubjects must necessarily give up some of their privacy in order to benefit from improved system security and functionalities. In this way, privacy is often "trumped" by more pressing social, legal, and economic imperatives; adding privacy to the system means subtracting something else. This is the classic "zero-sum" thinking.

Zero-Sum Security?

I am deeply opposed to the common view that privacy is necessarily opposed to, or an obstacle to, achieving other desirable business, technical or social objectives. For example:

- Privacy versus security (which security? informational, personal or public/national?)
- Privacy versus information system functionality
- Privacy versus operational or programmatic efficiency
- Privacy versus organizational control and accountability
- Privacy versus usability

The zero-sum mentality manifests itself in the arguments of technology developers and proponents, vendors and integrators, business executives and program managers – that individual privacy must give way to more compelling social, business, or operational objectives.

At the same time, defenders or advocates of privacy are often cast, variably, as Luddites, technological alarmists, or pressure groups largely out of touch with complex technological requirements and organizational imperatives.

Because of this prevailing zero-sum mentality, a proliferation of surveillance and control technologies are being deployed, without appropriate privacy checks and balances.

I am making the case for building privacy into information technology systems at any early stage, not only because failing to do so can trigger a public backlash and a "lose-lose" scenario, but because doing so will generate positive-sum benefits for everyone involved, in terms of improved compliance, user confidence and trust.

Better still, building privacy into invasive information and communications surveillance technologies may be accomplished *without* sacrificing data security, system functionality, efficiency, usability, or accountability.

Privacy-Enhancing Technologies (PETs)

Privacy, and specifically information privacy technologies, can transform zero-sum scenarios into positive-sum "win-win" scenarios.

The term "Privacy-Enhancing Technologies" (PETs) refers to "coherent systems of information and communication technologies that strengthen the protection of individuals' private life in an information system by preventing unnecessary or unlawful processing of personal data or by offering tools and controls to enhance the individual's control over his/her personal data." This concept also includes the design of the information systems architecture. Since 1995, when the IPC first coined the acronym, the concept and term have both entered into widespread vocabulary and use around the world.

PETs express universal principles of fair information practices directly into information and communications technologies, and can be deployed with little or **NO** impact on information system functionality, performance, or accountability.

Adoption of PETs increases user confidence, and makes it possible to apply new information and communication technologies in a way that achieves multiple objectives. When applied to technologies of surveillance, a PET becomes a transformative technology, which:

- Helps minimize unnecessary disclosure, collection, retention and use of personal data;
- Empowers individuals to participate in the management of their personal data;
- Enhances the security of personal data, wherever collected/used;
- Promotes public confidence and trust in (personal) data governance structures;
- Helps promote and facilitate widespread adoption of the technology.

Examples of Transformative Technologies

Biometric Encryption – BE offers viable prospects for 1:1 on-card matching of biometric and privacy-enhanced verification of identity in a wide range of contexts, helping to defeat unwanted identification, correlation and profiling on the basis biometric images and templates, as well as 1:N comparisons.

RFID – The IBM "clipped chip" is a consumer PET which helps to defeat unwanted surveillance. Similar innovations in user-centric RFID PETs have far-reaching consequences and commercial potential for use in RFID-embedded identity documents, payment tokens, mobile authentication, and other authorization form factors (e.g., transit fare cards, loyalty cards).

Private Digital Identity – Credentica (now Microsoft) developed minimal-disclosure digital identity tokens that work with major IDM platforms and help defeat unwanted correlation of user activities by online identity providers, without diminishing transaction accountability or control.

Video Surveillance – The Toronto mass transit video surveillance system will investigate the potential to deploy a privacy-enhanced encryption solution to prevent the unnecessary identification of passengers (see below).

Video Surveillance Cameras:
An Innovative Privacy-Enhancing Approach

At the University of Toronto, Canada Professor Kostas Plataniotis, and Karl Martin have developed a transformative privacy-enhancing approach to video surveillance. Their work, as described in "Privacy Protected Surveillance Using Secure Visual Object Coding,"[1] uses cryptographic techniques to secure a private object (personally identifiable information), so that it may only be viewed by designated persons of authority, by unlocking the encrypted object with a secret key. In other words, objects of interest (e.g., a face or body) are stored as completely separate entities from the background surveillance frame, and efficiently encrypted. This approach represents a significant technological breakthrough because by using a secure object-based coding approach, both the texture (i.e., content) and the shape of the object (see Figure (b) below), or just the texture (see Figure (c) below) may be encrypted. Not only is this approach more flexible, but the encryption used is also more efficient than existing approaches that encrypt the entire content stream. This allows designated persons to monitor the footage for unauthorized activity while strongly protecting the privacy of any individuals caught on tape. Upon capture of an incident that requires further investigation (i.e., a crime scene), the proper authorities can then decrypt the object content in order to identify the subjects in question. The decryption can be performed either in real-time or on archived footage. Since the encryption is performed in conjunction with the initial coding of the objects, it may be performed during acquisition of the surveillance footage, thus reducing the risk of any circumvention.

Figure (a): original content stream; Figure (b): both shape and texture have been encrypted and, despite attempts to hack into this with an incorrect key, objects of interest could not be decrypted; Figure (c): example where only the texture of the whole body (or face) is encrypted.

The figure contains a photograph of one of the researchers. The researcher in the photograph consented to its publication in this Report.

1 See Karl Martin and Konstantinos N. Plataniotis, *"Privacy protected surveillance using secure visual object coding"*, the Edward S. Rogers Sr. Dept. of Electrical and Computer Engineering, University of Toronto, Multimedia Lab Technical Report 2008.01 online: **http://www.ipsi.utoronto.ca/Assets/News/Technical+report+mass+transit+system+surveillance.pdf**

Published: March 2009

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Canada

Telephone: 416-326-3333 • 1-800-387-0073
Facsimile: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca
Email: info@ipc.on.ca