CONTACT INFORMATION:

General inquiries should be directed to:
Tel: (416) 326-3333
1-800-387-0073
Fax: (416) 325-9196
TTY (Teletypewriter): (416) 325-7539
e-mail: info@ipc.on.ca
Website: www.ipc.on.ca

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

Ann Cavoukian, Ph.D.
INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO
CANADA
Ann Cavoukian, Ph.D.
Information and Privacy Commissioner of Ontario, Canada
For many years, I have argued that privacy is part of the essential foundation upon which free and democratic societies are built. Our right to control the collection, use and disclosure of information about ourselves is the right upon which our other freedoms – freedom of association, freedom of movement, and the freedom to live as we choose – rest. Therefore, to preserve our privacy is to preserve that which we cherish but often take for granted – the freedom and liberty that define the open society in which we live.

It is this understanding that has fuelled my longstanding interest in the privacy rights of individuals, and that has so powerfully cemented my dedication to the cause.

Over the years, I’ve seen many developments in the world of privacy. I’ve also seen the world change in ways that no one could have anticipated, even 20 years ago. And with these changes – the growing deployment of biometrics, Radio Frequency Identification, online social networks, and cloud computing, among many others – have come new challenges to privacy and our ability to exercise that right effectively.
But unlike some critics, who see technology as necessarily eroding privacy, I have long taken the view that technology is inherently neutral. As much as it can be used to chip away at privacy, its support can also be enlisted to protect privacy through the use of Privacy-Enhancing Technologies (PETs) – a term that I coined in 1995 with the Netherlands Data Protection Authority. The concept of PETs was predicated on a deeper philosophy – that of embedding privacy into the design specifications of technology itself, thereby ensuring its ongoing presence.

Even in the ’90s, it was clear to me that the time was upon us when regulation and policy would no longer be sufficient to safeguard privacy. With the increasing complexity and interconnectedness of information technologies, nothing short of building privacy right into system design, in my view, could suffice. So I developed the concept of “Privacy by Design” to capture the notion of embedding privacy into technology itself – making it the default, delivered through various PETs. At that time, this approach was considered to be quite controversial. Now, it is the status quo.

Recently, I’ve evolved the concept of PETs, extending it to “PETs Plus,” by adding one new component – a positive-sum paradigm. The prevailing zero-sum model, wherein privacy is pitted against security, or against business practices, is destined to fail – including the failure of privacy. But if you change the paradigm to an inclusive positive-sum model, which allows the growth of both privacy and security, hand-in-hand, then the future of privacy grows more certain. PETs Plus recognizes the role of infrastructure, design, and architecture in enhancing privacy and building user confidence and trust. Take this a step further and you can achieve what I am calling Transformative Technologies, which have the power to transform otherwise privacy-invasive technologies into privacy-protective ones – positive-sum all the way.

These evolutions have arisen as our rapidly changing world has called into question the prevailing views of how best to protect privacy, now and well into the future. A key characteristic of these evolutions is that they recognize that individual control will play a lesser role in the protection of personal information. With Web 2.0 providing users with fewer and fewer touch-points, controls must become an inherent part of the system.

What has remained constant throughout these evolutions is my firm conviction that a future without Privacy by Design – a future where privacy is not integrated thoughtfully and consistently into the very fabric, the very architecture of technology itself – is a future in which privacy will cease to exist. And with that, many of the fundamental freedoms that we now take for granted, will also begin to erode.

This anthology pulls together some of my Office’s most important work in the area of Privacy by Design. It’s an area we’ve been particularly active in over the past two years as some new technologies, like RFID and online social networking, have
Introduction

exploded onto the scene, raising questions about how they may be deployed in a privacy-protective manner.

In the course of our work, we’ve been fortunate to form some strong partnerships, working closely with leading organizations such as IBM, Intel, Hewlett-Packard and Facebook to build awareness and encourage the development of responsible approaches to technology. The results of some of these partnerships appear in this anthology.

I fully expect that over the coming years my Office will continue to be active in encouraging the development and uptake of PETs Plus. But as our environment becomes more complex, and the threats to privacy increasingly difficult to pinpoint, the path ahead points toward an integrated and expansive model of Privacy by Design.

Whereas our focus has, until now, largely been on building privacy into information technologies, we have now begun to work more closely with organizations, both public and private sector, to also build privacy tools into business practices and into physical design. From data breach protocols to the layout of hospital waiting rooms, opportunities abound to treat privacy as a design concept from the outset, and to achieve privacy objectives alongside other operational goals.

I call this the Privacy by Design Trilogy, and it is my sincere hope that this direction will cement the idea that privacy interests do not operate in a zero-sum model. We need not trade off privacy against other goals like security or transparency. Having more of one does not necessitate having less of the other – quite the opposite. It is indeed possible, desirable, and feasible to have both. And I believe we can do that with the careful application of the principles of Privacy by Design laid out in the pages that follow.

Whatever field you work in or whatever technologies you interact with, I hope that you find the papers collected here to be thought-provoking, and I encourage you to consider ways in which privacy and technology can interact. While this is a small sample of the work that my Office has done, it is perhaps our best. You will find our remaining resources at www.ipc.on.ca. Here’s to privacy and freedom – living well into the future.

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner of Ontario, Canada
# Table of Contents

## Introduction
- General Introduction iii
- Privacy by Design 1
- Commissioner Ann Cavoukian Rolls Out the “Big Guns” to Prove Her Point about Using Technology to Protect Privacy: *The Privacy by Design Challenge* 9
- Privacy and Radical Pragmatism: Change the Paradigm 13
- Moving Forward from PETs to PETs Plus: the Time for Change is Now 41

## Transformative Technology

1. **CCTV Surveillance Cameras**
   - Transformative Technologies Deliver Both Security and Privacy: Think Positive-Sum, Not Zero-Sum 49
   - Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report 57

2. **Biometrics**
   - Biometric Encryption: A Positive-Sum Technology That Achieves Strong Authentication, Security, and Privacy 109

3. **RFIDs (Radio Frequency Identifiers)**
   - Privacy Guidelines for RFID Information Systems (RFID Privacy Guidelines) 147
   - RFID and Privacy: Guidance for Health-Care Providers 155
   - Adding an On/Off Device to Activate RFID Tags in Enhanced Driver’s Licences: Pioneering a Made-in-Ontario Transformative Technology That Delivers Both Privacy and Security 195
   - The Commissioner's Remarks to the Standing Committee of the Legislature of Ontario Regarding Bill 85, to Create an Enhanced Driver's Licence 201
4. Whole Body Imaging
   • Increase Airport Security Without Compromising Privacy: Commissioner Cavoukian Makes the Case for the Use of “Privacy Filters” 213
   • Whole Body Imaging in Airport Scanners: Activate Privacy Filters to Achieve Security and Privacy 217

Web 2.0
   • 7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity 229
   • Privacy in the Clouds: A White Paper on Privacy and Digital Identity 247
   • Privacy and the Open Networked Enterprise 265
   • The New Federated Privacy Impact Assessment (F-PIA): Building Privacy and Trust-Enabled Federation 299

Online Social Networks
   • Online Privacy: Make Youth Awareness and Education a Priority 329
   • How to Protect Your Privacy on Facebook: A Step-by-Step Guide 339
   • Reference Check: Is Your Boss Watching? Privacy and Your Facebook Profile 345
Privacy by Design

January 2009
I first developed the term “Privacy by Design” back in the '90s, when the notion of embedding privacy into the design of technology was far less popular. At that time, taking a strong regulatory approach was the preferred course of action. Since then, things have changed considerably. This paper summarizes the meaning and origins of Privacy by Design – an approach that is now enjoying widespread currency.

What Is Privacy by Design?
In brief, Privacy by Design refers to the philosophy and approach of embedding privacy into the design specifications of various technologies. This may be achieved by building the principles of Fair Information Practices (FIPs) into the design, operation and management of information processing technologies and systems. This approach originally had technology as its primary area of application, but I have since expanded its scope to two other areas. In total, the three areas of application are: (1) technology; (2) business practices; and (3) physical design.

As a broad overarching concept, Privacy by Design encompasses many elements in practice:

1. Recognition that privacy interests and concerns must be addressed;
2. Application of basic principles expressing universal spheres of privacy protection;
3. Early mitigation of privacy concerns when developing information technologies and systems, across the entire information life cycle;
4. Need for qualified privacy leadership and/or professional input; and
5. Adoption and integration of privacy-enhancing technologies (PETs).

IPC Advocacy of Privacy by Design
My office has been engaged in promoting all of these elements for many years.

1. Recognizing the benefits of addressing privacy interests and concerns
Privacy by Design begins with the understanding of both the value and benefits of adopting good privacy practices. In the mid-'90s, publications by the Office of the Information and Privacy Commissioner of Ontario (IPC), such as Privacy Protection Makes Good Business Sense and Privacy: The Key to Electronic Commerce, argued that all organizations that collect, use and disclose personal information should proactively accommodate the privacy interests and rights of individuals throughout their operations. More than a moral imperative, respecting privacy offered positive-sum dividends to all concerned. The “payoff” to organizations would come in many ways, including: improved customer satisfaction and trust;
enhanced reputations; reduced legal liabilities; more efficient operations; commercial gains and enhanced ROI; and, ultimately, enduring competitive advantage.¹ Our mantra, of “Privacy is good for business,” has been – and continues to be – a central message that we have consistently advocated.

2. Applying universal principles of Fair Information Practices

In order to be effective and credible, building privacy into technologies and operations must be done in a systematic way, with reference to widely-agreed upon privacy principles, standards and other relevant guidance. From the earliest days, the IPC has advocated a principled approach to ensuring Privacy by Design. The principles of Fair Information Practices give practical expression to individual privacy rights and the obligations of organizations to observe them.

I have always argued that organizations should apply FIPs to their operations. Voluntary international FIPs, such as the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, have served as the blueprint for the development of national privacy laws, but in the mid-’90s the IPC began to recognize that they also inform the design of information systems. My office has long supported the OECD Guidelines and, subsequently, the CSA Model Code for the Protection of Personal Information when it was finalized in 1995 to provide “the Canadian context and the new challenges of privacy protection in the information age.”²

3. Privacy concerns must be identified and mitigated early and comprehensively

“Build in privacy from the outset” has been my long-standing mantra, to “avoid making costly mistakes later on, requiring expensive retrofits.” I have long advocated for the earliest and most iterative identification of privacy issues – preferably at the design stage, but also at the development and implementation stages. Volume II of the 1995 Privacy-Enhancing Technologies: The Path to Anonymity offers a flowchart and discussion of “how the designer can take the user’s privacy into account during the different phases of the design process.”

Perhaps the clearest expression of my early advocacy for this approach is found in my 1997 paper, Smart, Optical and Other Advanced Cards: How to Do a Privacy Assessment, which sets out a framework and methodology for building privacy into applications “right from the start.” The paper is notable for going beyond specific technologies to insist upon the need to address privacy systematically, at the policy and organizational levels. Privacy Impact Assessment (PIA) tools and similar guidance documents remain a mainstay of my office’s output to this very day.


² Privacy Protection Models for the Private Sector (Dec 1996):
www.ipc.on.ca/index.asp?layid=86&fid1=328
Ontario and Canadian governments have emerged as leaders in the development and adoption of PIAs for all projects involving personal information. This year, my office is advancing this further by developing the next generation of tools in this area, focused squarely on not only identifying, but also managing the risk to privacy. Our PRM, or Privacy Risk Management Tool, will be rolled out later this year.

4. **Involving dedicated and qualified leadership and professional input**

In our 1995 paper with the Netherlands Data Protection Authority, *Privacy-Enhancing Technologies: The Path to Anonymity*, I coined the term “PETs” and set out a principled approach to building privacy into identity technologies and systems. This was directed squarely at designers of information systems. Applying privacy design practices, features and standards requires increasingly specialized expertise, as information technologies and systems become more complex, and more critical to an organization’s operations.

At the same time, knowledge of the organization and of the related privacy subdomains (legal compliance, technology, business operations, customer relations) are also critical for successful Privacy by Design efforts. I have long advocated for dedicated and well-resourced Chief Privacy Officers (CPOs) or similar positions to be created in order to enable strong privacy leadership and accountability.

5. **Adoption and integration of privacy-enhancing technologies (PETs)**

The growth of computer applications, digitized data and networks into every aspect of our lives has brought novel and profound privacy concerns that cannot be ignored. Fortunately, technology can also help. From a privacy perspective, information and communication technologies (ICTs) are essentially neutral. What matters are the choices we make when designing and using them – ICTs can be privacy-invasive or privacy-enhancing, depending on their design. “Privacy-enhancing technologies” embody fundamental privacy principles by minimizing personal data use, maximizing data security, and empowering individuals. As mentioned earlier, PETs can be engineered directly into the design of information technologies, architectures and systems by, for example, “minimizing the identity domain” and “minimiz[ing] … personal data stored in a database.”

**Applied Privacy by Design**

By the mid 1990s, the Ontario Government had begun to adopt increasingly sophisticated information and communications technologies and systems, in an effort to benefit from the advantages offered by the emerging “Information Highway.”

Of course, the collection, use, sharing and retention of more and more personal information, made possible by large-scale IT projects, posed significant privacy issues.
Given my office’s oversight of provincial and municipal government operations, and my presence on privacy and technology issues, my office was increasingly being consulted by public and private sector organizations for advice and guidance on how, exactly, to build in privacy early on – at the design stage of these new systems.

What followed was a succession of joint collaborations on groundbreaking new technology-enabled projects that focused on developing and applying privacy design principles into the development process so that any privacy-invasive risks could either be minimized or eliminated altogether.

In 1997, we worked with the Smart, Optical and Advanced Card Industry to create a tool designed to help developers of applications using advanced card technologies to understand and implement, in a practical way, the principles of privacy protection.

That same year, we worked with the Ontario Transportation Capital Corporation to design privacy into the newly built electronic toll highway – Highway 407. The electronic toll surveillance system, used primarily for automatic billing purposes, also resulted in the world’s first “anonymous account billing system,” as a result of our intervention to address privacy related concerns.

In 1998-99, we developed a paper with the Dutch Registriekamer, setting out privacy design criteria for intelligent software agents, *Turning a Privacy Threat into a Privacy Protector*.

Perhaps our largest collaborative Privacy by Design project was with the United States Department of Justice, Office of Justice Programs, from 1999 to 2001. That effort resulted in the release of our *Privacy Design Principles for an Integrated Justice System* in 2000. This paper outlines a set of Privacy Design Principles that would apply to the design and implementation of an integrated justice system, including the criminal justice process, as well as civil court records, juvenile justice information, and probate proceedings. As we noted in the introduction: “This paper is intended to spark informed debate in two areas. The first centers on the Privacy Design Principles and their applicability at various points within the justice system. The second area of debate centers on how technology can be used to implement the design principle policy. In this area, the paper describes ‘technology design principles’ to help a Technology Design Architect implement the Privacy Design Principles.”

All of these elements came together later that year in *Privacy by Design: Building Trust into Technology*, my presentation to the 1st Annual Privacy and Security Workshop by the Centre for Applied Cryptographic Research (CACR).
The Future of Privacy is *Privacy by Design*

Since that time, my office has become ever more deeply involved in helping public and private sector organizations alike understand the importance and need for our *Privacy by Design* approach. We have done this through a long succession of advocacy, guidance, and collaborative initiatives that continues unabated, to this day. Indeed, if anything, it is accelerating!

This need has become ever more important as we enter into a period of accelerating development and adoption of new ICTs and the near-exponential growth in the creation, dissemination, use and retention of personal information. I believe it has become more critical now than ever to embrace the *Privacy by Design* approach. I am gratified that this call is being heard and answered around the world by privacy and data protection commissioners, technologists, engineers, computer scientists, private- and public-sector organizations, privacy advocates, and the public at large. May it grow, well into the future, thereby ensuring the future of privacy.
Privacy by Design

List of IPC Publications

Privacy Protection Makes Good Business Sense (October 1994):
www.ipc.on.ca/index.asp?layid=86&fid1=327

Privacy-Enhancing Technologies: The Path to Anonymity (August 1995): Volume I:
www.ipc.on.ca/index.asp?layid=86&fid1=329

Privacy-Enhancing Technologies: The Path to Anonymity (August 1995): Volume II:
www.ipc.on.ca/images/Resources/anoni-v2.pdf

Privacy Protection Models for the Private Sector (Dec 1996):
www.ipc.on.ca/index.asp?layid=86&fid1=328

Smart, Optical and Other Advanced Cards: How to Do a Privacy Assessment (Sept 1997):
www.ipc.on.ca/index.asp?navid=46&fid1=297

Privacy: The Key to Electronic Commerce (April 1998):
www.ipc.on.ca/images/Resources/e-comm.pdf

407 Express Toll Route: How You Can Travel the 407 Anonymously (May 1998):
www.ipc.on.ca/index.asp?navid=46&fid1=335

Intelligent Software Agents: Turning a Privacy Threat into a Privacy Protector (April 1999):
www.ipc.on.ca/images/Resources/up-isat.pdf (cf. s.5.6 PETs Design criteria for agents)

www.ipc.on.ca/index.asp?layid=86&fid1=318

www.ipc.on.ca/index.asp?layid=86&fid1=326

Privacy by Design: Building Trust into Technology. Presentation by Ann Cavoukian, Ph.D. to the 1st Annual Privacy and Security Workshop. Centre for Applied Cryptographic Research (CACR), Toronto, Ontario, Canada – November 10, 2000:
www.cacr.math.uwaterloo.ca/conferences/2000/isw-sixth/cavoukian.ppt
Commissioner Ann Cavoukian Rolls Out the “Big Guns” to Prove Her Point about Using Technology to Protect Privacy: The Privacy by Design Challenge

January 2009
Ontario’s Information and Privacy Commissioner, Dr. Ann Cavoukian, has been urging governments and businesses for many years to embed privacy into the design of new technologies. That’s why she brought in the big guns of the technology world to prove her point.

Among the 10 speakers at the Privacy by Design Challenge in Toronto on January 28, 2009 were leading executives from major companies such as Intel, IBM, Microsoft, HP, Sun Microsystems and Facebook, as well as emerging companies such as Peratech and Privacy Analytics, which are leading with innovative privacy technologies. The focus of the conference was on the emergence and growth of privacy-enhancing technologies (PETs), which the Commissioner believes will pave the way for ensuring the future of privacy.

The Commissioner, who co-sponsored the conference with the Toronto Board of Trade, selected January 28 as the date for this event in order to commemorate the international celebration of Data Privacy Day.

“In a world of increasingly savvy and inter-connected customers, an organization’s approach to privacy may offer precisely the competitive advantage needed to succeed,” said Commissioner Cavoukian. “Privacy is essential to creating an environment that fosters trusting, long-term relationships with existing customers while attracting opportunity and facilitating the development of new ones.”

Privacy by Design is a term the Commissioner coined in the ’90s when she began her campaign to enlist the support of technology companies to develop technologies that protect privacy, rather than encroach upon it. Since then, great progress has been made in this area, as evidenced by the 10 speakers who appeared at this event, wishing to showcase their privacy-protective technologies.

The guest speakers served on two five-person panels. Members of the first panel, and their topics, included:

- **Jeff Jonas**, Chief Scientist, Entity Analytic Solutions, IBM, spoke on “responsible innovations in advanced information systems”;

- **David Hoffman**, Director of Security Policy and Global Privacy Officer, Intel Corporation, focused on “protecting personal information on mobile computers”;

Commissioner Ann Cavoukian Rolls Out the “Big Guns” to Prove Her Point about Using Technology to Protect Privacy:

*The Privacy by Design Challenge*
Dr. Stefan Brands, Principal Architect, Identity & Security Division, Microsoft Corporation, focused on “progress on an open platform for claims-based identity”;

Chris Kelly, Chief Privacy Officer, Facebook, discussed using Facebook Connect to protect privacy on the Web; and

Victor Garcia, Chief Technology Officer, HP (Canada) Co., focused on “services which protect personal privacy and corporate data.”

Members of the second panel, and their topics, included:

Dr. Khaled El Emam, Chief Technology Officer, Privacy Analytics Inc., addressed “sharing sensitive data without compromising individual privacy”;

Eileen MacDonald, Chief Operating Officer, GS1 Canada, described their coordinating role in the development of an on/off switch for Enhanced Driver’s Licences;

Philip Taysom, Chief Executive Officer, Peratech Limited, demonstrated a technology which enabled on/off switches for Enhanced Driver’s Licences;

Michelle Dennedy, Chief Privacy Officer, Sun Microsystems, Inc., discussed “advances in thin client computing – a strategy that eradicates data on the end point, preventing audit and data spills”; and

Tom Marinelli, Chief Information Officer and Vice-President, Ontario Lottery & Gaming Corporation, presented an innovative use of “biometric encryption to protect privacy in a facial recognition system.”
Privacy and Radical Pragmatism:
Change the Paradigm

August 2008
Foreword

In the two decades that I have served as a privacy regulator, I have seen profound changes in the world of privacy, and have learned many lessons along the way. Over the years, I have continually attempted to refine my views, approaches and methods of advancing privacy.

Today, I believe that we stand on the cusp of powerful changes that are transforming our world, transforming the way that we organize our lives and relate to each other – changes wrought in part by developments in information and communications technologies.

Not surprisingly, privacy as a concept and a right is also changing, changes to which we must continually adapt. We must preserve the insights of the past and adapt to new contexts never contemplated in the early days by the framers of privacy laws.

Some say that privacy is fast becoming an outdated concept, a function more of default practical obscurity than of ongoing societal debate and consensus. I’m not one of those people. It’s hard to believe that, 20 years ago, the debate raged on for years about the privacy pros and cons of caller ID and, later, reverse telephone directories! Yet these technologies and features are commonplace today and accepted as the norm. No one seriously challenges them anymore – our ideas of the acceptable boundaries for privacy have evolved over time.

But in the words of Professor Fred Cate, the era of “ubiquitous data availability” is clearly upon us, and if privacy is to survive in future decades, then we must change the paradigm to adapt to this ever-shifting environment.

Enter “radical pragmatism” …

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner of Ontario
August 2008
Radical Pragmatism

This paper sets out my office’s vision, philosophy and approach to advancing information privacy in the 21st century. While providing a basis for action, our new doctrine of “radical pragmatism” is not intended in any way to conflict with our legislated mandate to uphold Ontario privacy and access to information laws in a fair, neutral and impartial manner. Rather, this document is intended to complement and strengthen them. Given that surveillance and privacy intrusion know no borders, we are proposing an approach that extends beyond jurisdiction – beyond legislated borders. We are proposing a practical, pragmatic approach, but one that should not be mistakenly equated with an acceptance of the status quo – it is precisely the opposite.

“Pragmatism” is an approach that evaluates theories or beliefs in terms of the success of their practical application.

“Radical” pragmatism (radical used here in the sense of “far-reaching” or “thorough”) is the embodiment of a positive-sum paradigm (explained below), involving taking a practical approach, and invoking the need for transformative technologies.

Taking a pragmatic approach requires that we understand not only the potential harm of a surveillance technology, but also the proposed benefits. We must then work to incorporate a positive-sum, privacy-enhancing paradigm to decrease the harm to privacy, and to achieve the benefits that the technology in question was designed to deliver – positive-sum, not zero-sum.

Creating Positive-Sum Solutions

The hallmark of radical pragmatism is its emphasis on creating positive-sum solutions – the opposite of zero-sum. In a zero-sum paradigm, which is often the prevailing view, privacy is regarded as an impediment standing in the way of innovation and desired goals. We will use security and surveillance technologies to illustrate the practical application of this approach.

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; either/or. 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, I do not believe it is advisable that privacy advocates reject all forms of technology possessing any surveillance capacity, overlooking their growing applications and potential benefits. This has not worked in the past and is unlikely to work in the future.
If anything, the concerns for public safety and security, in a world gripped by the fear of terrorism, are not decreasing. Similarly, in the world of business, the call for privacy is often muted if it translates to a decrease in efficiency, in an age of global competition. This is the empirical evidence we are faced with from the last two decades.

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, serves to enhance the overall design. A positive-sum paradigm describes a situation in which all participants may gain together (win-win).

To achieve a positive-sum model, privacy must be proactively built into the system, so that privacy protections are engineered directly into the technology, right from the outset. I call this “privacy by design”. The effect is to minimize the unnecessary collection and use of personal data by the system, while at the same time, strengthening data security, and empowering individuals to exercise greater control over their own information. This can result in a technology that achieves strong security and privacy, delivering a “win-win” outcome.

**Transformative Technologies**

**Positive-Sum Paradigm + Privacy-Enhancing Technology**

*(Applied to a Surveillance Technology) = Transformative Technology*

By adopting a positive-sum paradigm and applying a privacy-enhancing technology to an otherwise surveillance technology, you can develop, what I am now calling, a “Transformative Technology” – transformative because you can in effect, transform the privacy-invasive features of a given technology into privacy-protective ones. Among other things, transformative technologies can literally transform technologies normally associated with surveillance into ones that are no longer exclusively privacy-invasive in nature. Creativity will be a necessary condition for such a positive-sum climate, as well as boundless innovation in technology. One form that such innovation may take is the development of intelligent agents in information systems, which have been “evolved” to do double duty: strongly protect one’s personal information and disclose it only for the purpose intended, according to a strict rule structure – in effect, transforming your personal data into what one enterprising researcher has called “Smart Data”.1 This will serve to minimize the unnecessary collection, use and disclosure of personal data, and ultimately promote public confidence and trust in data governance structures.

---

1 Dr. George Tomko, Expert-in-Residence, IPSI, University of Toronto, July 27, 2008.

http://www.ipc.on.ca/index.asp?navid=46&fid1=784
"Privacy is dead or dying." This is an oft-repeated phrase that more and more people are proclaiming as they contemplate the information technology and social revolutions that are transforming our world.

In the existing Information Era, all the rules appear to be changing. Thanks to the advent of more powerful, cheaper and cost-effective sensors, processing capabilities, communications links, and storage capacity, we are collectively creating, using, transmitting, and storing personal data at near-exponential rates of increase.

Practical obscurity – the basis of privacy since time immemorial – is fast disappearing and, in the words of Professor Fred Cate, we are moving toward a world of ubiquitous data availability.

At one time, the most serious threats to personal privacy came primarily from large centralized institutions, such as big governments and the media. The excesses of these institutions triggered society to pass corrective laws and put into place oversight mechanisms, such as defamation tort laws. Privacy became established as a distinct right and obligation, and as a justifiable limit to be placed on other rights.

Over time, with the advent of computerized record keeping, the privacy threats spread to a wider range of industries and organizations, and traversed boundlessly across jurisdictional boundaries. The errors and abuses of thousands of credit reporting firms in the 1960s and '70s led to devastating consequences for individuals seeking credit. Society reacted by extending oversight laws and mechanisms. The principles of Fair Information Practices were born, serving as a form of international DNA for thousands of privacy laws and codes of practice, entrenching rights of individuals to know of, and have a say in, the existence and management of their personal data, held by others. New oversight mechanisms were born to ensure that organizations kept their promises and abided by the rules imposed, and most important, did not use personal data in unauthorized ways.

Today, with the advent of Web 2.0 and the participatory Web, the environment is fast changing. The emerging approach to information management is fast becoming “search, don’t sort”; nearly anyone and everyone can be a data processor, collecting and using personal data in novel and unaccountable ways. The floodgates have been opened wide, with the data deluge threatening to overwhelm us. Our personal data appears to be everywhere, available to all, at any time, for any possible use, with a wide range of possible impacts.

It seems as if we’ve gone from Orwell’s 1984 to Franz Kafka’s The Trial. The dominant privacy threat today is no longer a single all-seeing entity bent on direct social control but, rather, the vast array of unknown and unaccountable entities that
may use our personal data and make decisions on that basis, toggling far-off levers and switches that can impact our lives in the most subtle ways. 24/7 surveillance, profiling, discrimination, identity theft and other misuses of our personally identifiable information (“PII”) have become endemic. Many are fast forgetting what privacy is, or why it is vital to preserving our freedom and liberty. The public is fast forgetting to what extent our privacy expectations are indeed reasonable.

**Surveillance Technologies**

Whether real-time or off-line, we are all increasingly under surveillance as we go about our daily lives. Surveillance control technologies generally include:

- 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); and
- 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 the behavior of individuals, surveillors may learn a great many new things about them which were never intended, and use that knowledge in misguided ways, potentially making discriminatory decisions affecting the individual.

The objectives of monitoring and surveillance, however, may be quite justifiable and beneficial at times. The essence of the problem is the zero-sum paradigm upon which such technologies are often based. The basic proposition of many surveillance systems is that users/subjects 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 what are considered to be more pressing social, legal, and economic imperatives. Under the present design, adding privacy to the system usually means subtracting something else. This is a classic “zero-sum” paradigm.
Zero-Sum Security?

Not only do I disagree with the common view that privacy is necessarily opposed to, or presents an impediment to, achieving other desirable goals such as business or technical objectives, but I also think this view is no longer sustainable.

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

For example, it is not uncommon to see:

- Privacy versus security
- Privacy versus information system functionality
- Privacy versus operational efficiency
- Privacy versus organizational control
- Privacy versus usability

At the same time, privacy advocates are inaccurately cast at times as either Luddites, technological alarmists, or members of pressure groups largely out of touch with the complex technological requirements and organizational imperatives.

Due in part to this prevailing zero-sum mentality, however, a proliferation of surveillance technologies are being deployed without the appropriate privacy checks and balances.

I continue to make 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 also because doing so will generate positive-sum benefits for everyone involved, in terms of greater privacy, improved compliance, user confidence and trust.

Better still, I believe that architecting privacy directly into invasive surveillance technologies may be accomplished without needing to sacrifice data security, system functionality, efficiency, usability, or accountability.

Really ... how? Enter radical pragmatism ...
Foundations of Radical Pragmatism

Radical privacy pragmatism does not represent a rearguard action or an acceptance of the status quo. It is not a last-gasp Utopian stand or inspirational but Quixotic call to action². Nor is it a Cassandran prophecy of doom or requiem for privacy in the 21st century. It is a call to action.

Radical pragmatism is both optimistic and realistic, principled and passionate yet calculating, inclusive and utilitarian, infused throughout with the resolve and energy needed to ensure that privacy continues to endure and flourish in coming generations. Radical pragmatism explicitly recognizes that privacy is not an absolute right or value but rather, a social value that is continually defined, determined and enforced by society, through informed discourse and dialogue and, yes, at times, dare I say it, “balance”. Like John Stuart Mill, I believe that privacy values and its benefits are best achieved through open public discourse and social dialogue – a thorough airing of all interests and views.

Radical pragmatism is consistent with the work of my office over the past 20 years. Indeed, it builds squarely upon the foundations of our work:

“Privacy is not just a policy issue or a compliance issue – it is a business issue, at the heart of the new economy.”³

The “Privacy Payoff”

The business case for privacy focuses, in essence, on gaining and keeping customer trust, loyalty, repeat business, and avoiding “churn.” The value proposition typically breaks down as follows:

1. Consumer trust drives successful customer relationship management (CRM) and lifetime value … in other words, revenues;

2. Broken trust will result in a loss of market share, loss of revenue, and lower stock value;

3. Consumer trust hinges critically on the strength and credibility of an organization’s data privacy policies and practices.

---

² Wikipedia defines “Quixotism” as “the description of a person or an act that is caught up in the romance of noble deeds and the pursuit of unreachable goals. It also serves to describe an idealism without regard to practicality. An impulsive person or act can be regarded as quixotic. Quixotism is usually related to “over-idealism”, meaning an idealism that doesn’t take the consequences into account. It is also related to naïve romanticism and to utopianism.”

³ The Privacy Payoff: How Successful Businesses Build Customer Trust, Ann Cavoukian, Ph.D. and Tyler J. Hamilton www.privacypayoff.com
The “privacy payoff” also works in reverse, that is, poor privacy can result in additional costs and foregone opportunities and revenues. A lack of attention to data privacy can result in a number of negative consequences:

- harm to clients or customers whose personal data is used or disclosed inappropriately;
- damage to an organization’s reputation and brand;
- financial losses associated with deterioration in the quality or integrity of personal data;
- financial losses due to a loss of business or delay in the implementation of a new product or service due to privacy concerns;
- loss of market share or a drop in stock prices following negative publicity;
- violations of privacy laws; and
- diminished confidence and trust in the industry.4

Thanks in part to growing breach disclosure laws, the collection, use and sharing of high volumes of personal information are becoming subject to greater scrutiny by the public and regulators alike. Organizations are being punished both in the marketplace and in the courts, for negligent personal information management practices – especially where the costs of their behaviour are borne by others (negative externalities).

At times, due to the actions of a few, many people are forced to suffer, with consumer confidence, trust and revenues being eroded for entire industries (such as the marketing, financial and e-commerce sectors). Many studies have demonstrated the “loss” or “unrealized potential” of businesses arising from consumer privacy and security concerns, especially online.

This is why adopting proactive privacy stances can provide market differentiation and lasting competitive advantage.5 Not only is this a matter of law and regulatory compliance but, equally important, customers expect it. Then add equal parts of responsible information management, transparency, governance and accountability and the governance structure is further enhanced. The privacy payoff is real.

---

4 For a greater discussion, see the IPC Publication, Privacy and Boards of Directors: What You Don’t Know Can Hurt You, at www.ipc.on.ca/docs/director.pdf
5 The Privacy Payoff: How Successful Businesses Build Customer Trust, Ann Cavoukian, Ph.D. and Tyler J. Hamilton. www.privacypayoff.com
In the words of one marketing consultant (2001):

“One thing is certain: Technological advances will force changes in the laws around the globe that protect privacy. If you wait for these changes to become obvious, you will forfeit a powerful competitive advantage. People trust leaders, not followers. Once legislation creates new standards for appropriate behavior, the public will be drawn to companies that can claim to have followed such standards before they were mandatory.”

“Privacy by Design” – Build It in Early On

As noted above, I believe that organizations will be rewarded for innovative, far-sighted and diligent information management practices that demonstrate a sustained commitment to privacy principles. Helping organizations achieve this in a practical manner is an important part of my office’s mandate and work.

For this reason, I have long advocated building privacy into the design and operation of information technologies and systems, at an early stage. The benefits of “privacy by design” are many. Besides being a valuable organizational due diligence exercise, it helps obviate the need for expensive systems design changes and retrofits later on, after an ill-fated disaster has occurred.

Privacy considerations may even lead to significant efficiencies and savings arising from simpler and more trustworthy design architectures.

The benefits of good “privacy by design” may at times be hard to measure, since the reduction of risk is not always easily quantifiable. What is the future discounted value of a privacy disaster that did not happen because of adequate foresight and action? The growing trend toward the public reporting of privacy and security breaches is adding another incentive to avoiding secrecy and negligence, to demonstrating due care and attention to privacy issues, and to “getting it right” the first time around.

Many of my office’s efforts have been focused on ensuring that privacy issues are fully identified, addressed and integrated into other corporate initiatives, such as IT security, corporate governance, “e-initiatives” and similar organizationally transformative changes, marketing, supply chain management, and so forth. In many cases, the (economic) benefit of good privacy emerges when it enables the benefits or prevents the excesses of other systems.

6 Bruce Kasanoff, Making it Personal: How to Profit from Personalization Without Invading Privacy (Perseus, October 2001), p.65.
Privacy-Enhancing Technologies (PETs)
The term “Privacy-Enhancing Technologies” (PETs) refers to “coherent systems of information and communication technologies that strengthen the protection of an individual's 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 we first coined the acronym, the concept and term have both entered into widespread use and added to the privacy vocabulary around the world.

PETs express the embedding of universal principles of fair information practices directly into information and communications technologies, and may 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 ways that achieve multiple objectives. When applied to technologies of surveillance, in a positive-sum paradigm, a PET becomes a transformative technology, which:

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

Over the years, I have shone the spotlight on many promising PETs in an effort to raise greater awareness, and to support their development and widespread adoption. At first, PETs were primarily tools for the exclusive use of individuals, such as personal e-mail and file encryption, online anonymizers and password managers. Over time, however, there has been growing emphasis on network or system-level PETs that help to enable personal privacy, such as the Platform for Privacy Preferences (P3P) standard, the 7 Privacy-Embedded Laws of Identity for the creation of an interoperable identity infrastructure, and various organization-centric data minimization tools.

As we will note later in this paper (in the case examples), many new and emerging Privacy-Enhancing Technologies involve actions by both the organization and the individual, and may be said to be truly transformative.

Best Practices in Information Management and Governance

The pragmatic approach that my office has taken over the years is also manifest in a number of other ways.

We have engaged a wide variety of organizations and associations in articulating, developing and adopting industry best practices in privacy self-evaluation, deploying effective data security and access controls, encryption, radio frequency identification, direct marketing, smart card development, federated identity, appointment of a chief privacy officer, and promotion of audit and assurance methods.

Considerable effort has also been invested in raising public awareness and education among all privacy stakeholders, from making available privacy tutorials for use in primary and secondary schools to publishing tip sheets on how to protect your privacy for Facebook users, offering assistance to identity theft victims, to discussion papers on critical issues for the public at large, through to advice for government agencies on deploying PKI and implementing a breach crisis plan.

All of these education and awareness materials and many more are available on my website – messages which are also delivered through other avenues such as speeches, presentations, media interviews and special events.

Privacy rights and protections do not exist in a vacuum, nor are they derived solely from laws and regulations. Without broad-based support and demand from society at large, privacy laws, policies and technologies will be for naught.

I am constantly scanning the environment, engaging in dialogue with the widest possible variety of societal actors and interests in order to stay current, relevant and effective at the most granular, pragmatic levels.

Radical pragmatism places a strong emphasis on strategic intervention and manipulation of the levers available in a co-ordinated and timely way to achieve optimal privacy outcomes, ideally without the need for confrontation and conflict, scapegoating, or heavy-handed intervention.
Applied Radical Pragmatism

What radical pragmatism is NOT:

- a harms-based approach
- a sellout to business or government interests
- technological Utopianism

Radical pragmatism involves a strategic focus of efforts on areas of high-risk and early opportunity.

It involves a return to the very basis and essence of privacy and data protection principles, namely, to reconcile overlapping and, at times, competing interests over the use of personal data, be it for public or commercial use.

Remember that privacy and data protection laws have always had dual purposes: while seeking to recognize the rights of individuals to protect them from harm, such laws also seek to ensure the free and uninterrupted (but responsible) flow and uses of personal data; to promote business and commerce; to ensure that public agencies are held accountable for their actions; and, more generally, to ensure that personal data is collected, used, retained and shared in a manner that is open, transparent, equitable, in accordance with the interests of individuals and, above all, to serve redeemable ends, be it improving efficiency, delivering new and innovative services, promoting competitiveness and quality care, ensuring operational efficiency and continuous improvement, or catching criminals.

The importance of ongoing dialogue and engagement cannot be overemphasized. Constant dialogue and understanding of the real world is an essential *sine qua non.*

The importance of strategic and tactical effectiveness, leveraging limited resources for the greatest possible effect, must also be recognized and valued.

We are supportive of technology and innovation, provided that privacy is built in, and features prominently.

In pursuing radical pragmatism, we seek the *Art of the Possible.*
Examples of Transformative Technologies

So, how is radical pragmatism actually applied in practice? As noted earlier, there is less of an emphasis on legal and regulatory compliance measures, and more focus upon the adoption of PETs, the voluntary adoption of best practices, and heightened awareness efforts. Needless to say, all legislated, regulatory measures must be adhered to.

This section examines a number of leading-edge technologies:

1. Biometric Encryption
2. IBM’s “Clipped-Tag” RFID
3. CCTV image encryption
4. Privacy-enhanced network tracing and monitoring
5. Whole body imaging
6. Private digital identities

1. Biometric Encryption

During the past decade, we have witnessed a rapid evolution and maturation of biometric technologies. Biometrics are now being deployed in a wide range of public and private sector uses and applications, including: physical and logical access controls; attendance recording; payment systems; crime and fraud prevention/detection; and border security controls.

Biometrics promise many benefits, including stronger user authentication, greater user convenience, and improved security and operational efficiencies. However, the data privacy and security concerns associated with widespread use of biometric technologies and the collection, use, and retention of biometric data are profound and significant, and include:

- unauthorized secondary uses of biometric data (function creep);
- expanded surveillance tracking, profiling, and potential discrimination;
- data misuse (data breach, identity fraud and theft);
- negative personal impacts of false matches, non-matches, system errors and failures;
- diminished oversight, accountability, and openness of biometric data systems; and
- absence of individual knowledge and consent; loss of personal control; loss of trust.
Significant data security risks are also present throughout the information life cycle, including: spoofing; tampering; replay, substitution, masquerade and Trojan horse attacks; overriding yes/no response; and insufficient accuracy.

Efforts to minimize identified privacy and security risks to acceptable levels and to encourage user confidence include strengthening legal and regulatory oversight mechanisms, developing clear data usage policies, and improving awareness, education, and training. These policy controls to protecting privacy in biometric systems can be supported by structural approaches, such as by limiting the design and operation of biometric technologies to authentication (1:1) rather than identification (1:n) purposes, and avoiding the creation of large centralized databases of biometric data, and encrypting biometric data at rest and in transit.

These are worthwhile efforts, but I have advocated going further to develop and deploy privacy-enhancing technologies, which enable individuals to manage their own personally identifiable information (PII) and minimize privacy risks at an earlier, more granular level.

Proponents of biometrics suggest that deploying PETs would hinder the objectives and functions of biometric-enabled information systems and applications. But this view is based on the common assumption, belief or argument that individual privacy must necessarily be sacrificed to broader societal, programmatic and operational needs, for example, accountability and security.

In my view, engineering privacy into (biometric) information systems is not only desirable and possible, but can also be accomplished in a way that achieves positive-sum results for all stakeholders. Biometric Encryption (BE) technologies are a good example of how privacy and security can both be increased together in a positive-sum model.

In brief, Biometric Encryption is a process that securely binds a PIN or a cryptographic key to a biometric, so that neither the key nor the biometric can be retrieved from the stored template. The key is recreated only if the correct live biometric sample is presented on verification. BE is a true PET. The technology is already being deployed in European and Asian pilot projects.

Some of the key benefits and advantages of BE technology include:

- No retention of the original biometric image or template;
- From the same biometric, multiple and unlinkable identifiers for different uses can be generated that are cancellable and revocable;
- Improved authentication security: stronger binding of user biometric and identifier;
- Improved security of personal data and communications;
Greater public confidence, acceptance, and use; compliance with privacy laws; and

Suitable for large-scale applications.

These advantages and solutions are set out in greater detail in my paper Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy.\(^8\)

In sum, 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. Biometric Encryption technology is a fruitful area for research and has become sufficiently mature for broader public policy consideration, prototype development, and consideration of applications.

2. Radio Frequency Identification (RFID)

Radio Frequency IDentification tags are the next generation technology beyond barcodes. RFID tags contain microchips and tiny radio antennas and can be attached to products. They transmit a unique identifying number to an electronic reader, which in turn links to a computer database where information about the item is stored, along with time and location information. RFID tags may be read from a distance quickly and easily, making them valuable for managing inventory and supply chain logistics.

However, the growing practice of tagging consumer products also raises many privacy and security concerns, especially when the tagged items being scanned are linked to identifiable individuals. The prospect of hidden, unauthorized readers scanning the personal items we carry about with us – such as our prescription vials, clothing brands, styles and sizes, or books we are reading – without our knowledge or consent is deeply troubling. Worse, the potential for ongoing surveillance, profiling and discrimination based on RFID tags in our possession undermines public confidence and trust in the technology and how it is being deployed.

A number of solutions to the problem of RFID tag “data leakage” and unwanted surveillance have been proposed over the years, but few have taken hold due to cost, technical or usability factors. The most obvious solution is to simply remove or destroy the tag at the point of sale, but this may impair the ability to effectively return and restock those goods, verify recalled products, ensure continuous warranty coverage and product servicing, or even identify the product for special post-consumer processing or recycling.

8 Available at: www.ipc.on.ca/index.asp?navid=46&fid1=608&fid2=4
Perhaps the most promising consumer PET solution is the “clipped tag” RFID developed by IBM, which helps to defeat unwanted surveillance, thereby delivering greater privacy. 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).

3. Video Surveillance Image Encryption
Thanks to technological advances in sensors, processing, and networking capabilities, video surveillance cameras are being deployed in more and more places, providing multiple simultaneous digital feeds to remote centralized locations for viewing, storage, indexing, and further processing. Many feeds are on the Web. Their uses raise profound questions about surveillance and individual privacy.

However, when deployed in a transparent and accountable manner, video surveillance cameras can help achieve valid objectives, such as crime detection and preserving evidence in the event of an incident. Nonetheless, valid concerns remain about how the recorded images will be used, what assurances people may have that the images will not be used for unrelated, secondary purposes, and what recourse, if any, individuals have in the event of misuse.
Following our report and recommendations regarding the planned deployment of thousands of video surveillance cameras throughout the Toronto mass transit system, the City of Toronto will investigate the potential to deploy a privacy-enhancing encryption solution to prevent the unnecessary identification of passengers.

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*[^9], 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 may 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, the objects of interest could not be decrypted; Figure (c): example where only the texture of the whole body (or only a face for example) is encrypted.](image)

4. Privacy-Enhanced Network Tracing and Monitoring

Today’s Internet service providers (ISPs) gather network traces to perform network management operations, such as traffic engineering, capacity planning, threat analysis, and customer accounting. Unfortunately, collecting this data raises huge privacy issues—it can be used to track a person’s online activities, it can be lost, stolen, or it can even be sold to advertisers. Relying on internal procedures to protect this data is not enough; in a recent case, sensitive data regarding Canadian Internet users was stolen by an employee with legitimate access. Furthermore, sensitive data is often the target of legal action. Recently, Viacom served Google with a subpoena requiring them to turn over the viewing history of every YouTube user.

Researchers at the University of Toronto have created a technology called “Bunker” that allows ISPs to securely trace their networks. Bunker collects sensitive data from the ISP’s network and stores it in a tamper-resistant system. Bunker then aggregates this data to produce a set of user-specified reports that provide insight into the traced network without compromising user privacy. Bunker’s tamper-resistant design means that an attack on the system is more likely to destroy all of the contained sensitive data than to succeed in capturing it. By using Bunker, ISPs can enforce their privacy policy using technology and protect trace data from being subpoenaed.

5. Whole Body Imaging

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. Metal detectors alone are not sufficient for this task, as they are unable to detect explosives, plastic or ceramic weapons, or other contraband (such as narcotics). The problem facing security officials, then, is to be able to detect a wide range of concealed items in a minimally invasive manner. The solution that is currently being widely piloted is “whole body imaging.”

Whole-body imaging is able to reveal objects hidden underneath clothing, without the need for a physical pat-down or strip search. One such technology, called backscatter, accomplishes this with low dose X-ray radiation, equivalent to the background radiation experienced during two minutes of flight. By detecting elements with both low and high atomic numbers, backscatter is able to identify hidden metal and/or plastic weapons, explosives and drugs.

10 http://www.cbc.ca/money/story/2008/02/12/bell.html
12 The following published paper presents the high-level idea and a preliminary design of their system: www.cs.toronto.edu/~stefan/publications/hotnets/2007/sectrace.pdf
To ensure that privacy is protected in this process, the image generated by a backscatter scan is viewed in a remote location, by a trained security official who does not interact with the scanned individual, nor has any personal information about him or her. The image is encrypted before transmission, cannot be stored, printed or transmitted, and is deleted from the screen (and thus the computer) prior to the next scan being performed. Most important, concerns that the unclothed physical features of the individual could be viewed by the operator were also addressed with the application of a “privacy filter.” This filter is applied to the scanned image before it is viewed, transforming the raw image (Figure 1) into an outline in which only potential threats are highlighted (Figure 2).

![Figure 1: Sample raw backscatter image](image1)

![Figure 2: Backscatter image, after privacy algorithm applied](image2)

**6. Private Digital Identities**

Requests for identification are becoming more widespread, more frequent, more mandatory, and more subject to stronger forms of authentication. Organizations, both online and off, often have legitimate needs to know who you are, for accountability purposes and to protect against possible fraud.

However, unlike the off-line world where displaying your proof of age, for example, to qualify for a purchase or discount, does not result in a record being retained, in the online world your personal identification and authentication data are being recorded, transmitted and retained. The potential for over collection of personal information and subsequent loss, theft, and misuse of sensitive personal data is significant, and is having an impact on public confidence in the Internet as a viable medium for trusted transactions.

Worse, the online world – again unlike the off-line world – poses significant risks that one’s identity credentials, when used across different domains, can be easily and quickly linked together to create highly detailed transaction profiles. It is well known that users’ behavior on the Web is the most intensely recorded and tracked of all interactions, and this surveillance is made possible through systems of identification.
Fortunately, innovative “user-centric” identification technologies have been developed in Canada by Credentica (since purchased by Microsoft) that allow online users to present online identity credentials that reveal absolutely no more information than is strictly necessary. The U-Prove product enables organizations to protect identity-related information with unprecedented security throughout its life cycle, wherever it may travel. It is tailor-made for online user authentication that must withstand phishing attacks, sharing identity information across disparate domains, and creating the digital equivalent of the cards in one’s wallet.

At the same time, the U-Prove product enables critical privacy functions. For example, it enables online users to seamlessly authenticate to any number of sites without giving rise to unwanted profiling or surveillance capabilities, transfer data between unlinked accounts, and store digitally signed audit trails that prove the veracity of the transactions they engaged in. These functions have been specifically designed to meet data protection requirements.

The success of large-scale information technology initiatives depends critically upon their public acceptance and use. In order for this to occur, the public must have confidence and trust in the data privacy and security claims being made. Credentica’s innovative U-Prove product promises to do this by giving users the ability to minimize the collection and use of their personal data in online transactions, and to maintain control over their identities. U-Prove is a true transformative technology, enabling both privacy and authentication of identity – positive-sum, and radically pragmatic.

13 Details at: http://www.credentica.com/
Endnote: Commissioner’s Message

As a regulator, I have been called many things during my tenure, but rarely have I been called a dreamer. But that is precisely the practice one must engage in if privacy is to not only survive, but thrive, well into the future. That is my hope and dream. But dreaming is not enough. As a pragmatist, I must embed that dream into reality. As I noted earlier, one way of doing so is seeking to embed privacy into the design and architecture of all technologies, so that it may live well into the future. After all, I am a radical pragmatist and I dream BIG – in technicolor, because there is no black and white any more. I invite you to join me in finding new ways of pragmatically embedding privacy into our day-to-day lives. I would be delighted to receive any examples that you send to me and the best of them will be posted on our website under “Instances of Radical Pragmatism.”

Let the list grow long, and let privacy grow strong – that is my dream. Let’s make it real.

Ann Cavoukian, Ph.D.

The Commissioner would like to gratefully acknowledge the excellent contribution of Fred Carter, Senior Privacy & Technology Advisor, Office of the Information and Privacy Commissioner of Ontario, in the preparation of this paper.
IPC References

Biometric Encryption
How to Preserve Freedom and Liberty: Design Intelligent Agents to be Smart and Respectful of Privacy (George Tomko, Ph.D. – IPSI Seminar, University of Toronto). October 2008.
http://www.ipc.on.ca/index.asp?navid=46&fid1=784

http://www.ipc.on.ca/index.asp?navid=46&fid1=769

http://www.ipc.on.ca/index.asp?navid=46&fid1=608&fid2=4

• News Release: http://www.ipc.on.ca/index.asp?navid=55&fid1=609
• Executive Summary:
  http://www.ipc.on.ca/images/Resources/up-bio_encryp_execsum.pdf
• FAQ: http://www.ipc.on.ca/index.asp?navid=46&fid1=608&fid2=4

Radio Frequency Identification (RFID)
http://www.ipc.on.ca/index.asp?navid=46&fid1=724


http://www.ipc.on.ca/index.asp?navid=46&fid1=432

http://www.ipc.on.ca/index.asp?navid=46&fid1=430

http://www.ipc.on.ca/index.asp?navid=46&fid1=410

Video Surveillance


http://www.ipc.on.ca/index.asp?navid=53&fid1=7874

http://www.ipc.on.ca/index.asp?navid=46&fid1=647

http://www.ipc.on.ca/index.asp?navid=46&fid1=626

http://www.ipc.on.ca/index.asp?navid=46&fid1=582

http://www.ipc.on.ca/index.asp?navid=46&fid1=412

Online Privacy

http://www.ipc.on.ca/index.asp?navid=46&fid1=748

http://www.ipc.on.ca/index.asp?navid=46&fid1=471

http://www.ipc.on.ca/index.asp?navid=46&fid1=339

Privacy and Digital Rights Management (DRM): An Oxymoron. October 2002
http://www.ipc.on.ca/index.asp?navid=46&fid1=241

http://www.ipc.on.ca/index.asp?navid=46&fid1=286

http://www.ipc.on.ca/index.asp?navid=46&fid1=403

Should the OECD Guidelines Apply to Personal Data Online? September 2000.
http://www.ipc.on.ca/index.asp?navid=46&fid1=246
Privacy by Design

http://www.ipc.on.ca/index.asp?navid=46&fid1=238

http://www.ipc.on.ca/index.asp?navid=46&fid1=345

Privacy and Security
http://www.ipc.on.ca/index.asp?navid=46&fid1=758

http://www.ipc.on.ca/index.asp?navid=46&fid1=575

http://www.ipc.on.ca/index.asp?navid=46&fid1=341

http://www.ipc.on.ca/index.asp?navid=46&fid1=113

http://www.ipc.on.ca/index.asp?navid=46&fid1=248

http://www.ipc.on.ca/index.asp?navid=46&fid1=236

http://www.ipc.on.ca/index.asp?navid=46&fid1=245

http://www.ipc.on.ca/index.asp?navid=46&fid1=333

Identity Theft
Identity Theft Revisited: Security is Not Enough. September 2005
http://www.ipc.on.ca/index.asp?navid=46&fid1=233
Miscellaneous

Contactless Smart Card Applications: Design Tool and Privacy Impact Assessment.
http://www.ipc.on.ca/index.asp?navid=46&fid1=614

http://www.ipc.on.ca/index.asp?navid=46&fid1=576

Incorporating Privacy into Marketing and Customer Relationship Management.
http://www.ipc.on.ca/index.asp?navid=46&fid1=234


http://www.ipc.on.ca/index.asp?navid=46&fid1=316

Volume I: http://www.ipc.on.ca/index.asp?navid=46&fid1=329
Volume II: http://www.ipc.on.ca/index.asp?navid=46&fid1=242

http://www.ipc.on.ca/index.asp?navid=46&fid1=325
Moving Forward from PETs to PETs Plus:
The Time for Change is Now

March 2009
Moving Forward from PETs to PETs Plus:  
The Time for Change is Now

Traditional PETs  
Privacy-Enhancing Technologies (PETs) refer to information and communication technologies (ICTs) that strengthen the protection of personal privacy in an information system by preventing the unnecessary or unlawful collection, use and disclosure of personal data, or by offering tools to enhance an individual’s control over his/her personal data.

PETs were developed in the '90s with the goal of enlisting the support of technology to enhance privacy, rather than encroach upon it. But the time has come to move the bar forward. PETs alone may at times be found to be lacking, which is why we have evolved the term to “PETs Plus.”

Since first coining the term “PETs” in 1995 with the Dutch Data Protection Authority, I have emphasized the need to incorporate the universal principles of Fair Information Practices (FIPs) directly into the design and operation of information processing technologies and systems as part of my “Privacy by Design” philosophy.

First codified by the OECD in 1980, FIPs come in a variety of flavours, including the E.U. Directive on Data Protection, Canada’s CSA Privacy Code, the Asia-Pacific Economic Cooperation (APEC) Privacy Framework, the U.S. Safe Harbor Principles, and, most recently, the harmonized Global Privacy Standard, which I led with international Privacy and Data Protection Commissioners, in 2006.¹

Despite minor differences, these FIPs all share the following fundamental common denominators:

- **Data minimization** – the collection, use, disclosure and retention of personally identifiable information should be minimized wherever, and to the fullest extent, possible;
- **User participation** – individuals should be empowered to play a participatory role and to exercise controls during the life cycle of their own personal data; and
- **Enhanced security** – the confidentiality, integrity and availability of personal data should be safeguarded, as appropriate to the sensitivity of the information.

¹ Cavoukian, Ann, Ph.D., Creation of a Global Privacy Standard (November 8, 2006):  
http://www.ipc.on.ca/images/Resources/gps.pdf
Traditional PETs promote user participation and empowerment

PETs should ideally promote all of these meta-principles. For example, an organization’s use of strong encryption technologies to secure detailed customer records against unauthorized access and use, while extremely valuable, in and of itself, speaks little to the data minimization and user participation requirements.

Traditional PETs contribute to the privacy ideals of informational self-determination, that is, an individual’s ability to exercise a measure of control over the collection, use and disclosure of their personal information. Given the history associated with the early developments of PETs in the 1990s, namely growing concerns with online surveillance issues, this is not surprising. As a result, online PETs have been typically defined to perform the following functions:

- preventing unauthorized access to communications and stored files;
- automating the retrieval of information about data collectors’ privacy practices and automating users’ decision-making on the basis of these practices;
- preventing automated data capture through cookies, HTTP headers, web bugs, spyware, etc.;
- preventing communications from being linked to a specific individual;
- facilitating transactions that reveal minimal personal information; and
- filtering unwanted messages.

These are user-centric tools and functions. The list has not been significantly lengthened in over a decade, and strongly suggests that PETs are discrete technologies that put individuals in greater control of their own personally identifiable information.

But have unnecessary boundaries been placed upon PETs? Are they cryptographic primitives, software or hardware applications, components embedded in larger systems, or entire information systems? Should PETs be understood to include only technologies under the exclusive control of the individual, or is there room for a more expansive definition that includes greater infrastructure components? The door must be widened.

PETs Plus

In widening the door, I felt that the concept of PETs had to be expanded. PETs Plus represents the evolution of PETs by adding a “positive-sum” paradigm to ICT designs and uses. The result is that PETs Plus seeks to achieve goals in addition to those intended to protect the interests of the individual alone. That is, PETs Plus facilitates achieving the goals of other participants or stakeholders such as, for example, those of the system owner and operator, in a positive-sum, not zero-sum model. These may be the functional and operational objectives of the system (e.g., to transport and route electronic communications, to process a payment, or provide a service), or other security, surveillance, and anti-fraud detection goals.
Again, these additional goals do not come at the expense of the individual (zero-sum), but in addition (positive-sum).

**PETs Plus recognize the importance of infrastructure**

How can PETs Plus achieve other goals in addition to privacy? By abandoning the prevailing zero-sum model of privacy vs. other interests. Not only is the zero-sum approach doomed to failure, but it is also the least efficient model to employ. The starting point should be the recognition that virtually all PETs possess an infrastructure component, in order to perform to their optimal level. For example: take a traditional PET, such as a software utility that individuals can download and install onto their computers to securely encrypt their files and email messages. In order for it to function, users must trust the embedded encryption algorithms to do their magic – that the downloaded file will come from a reliable source and will be “clean” when installed. In order to securely communicate, other users must also have the same software program installed on their computers, and be able to connect, using appropriate infrastructures. To facilitate the exchange and lookup of (PKI) encryption keys, public key servers may need to be available, hosted by trusted parties, and so forth.

The same reliance upon infrastructure and other parties is also true for another quintessential PET, the Platform for Privacy Preferences (P3P), in which users can establish their machine-readable privacy preferences, which are then automatically matched against the privacy policies of participating websites visited. In order to have any privacy relevance or utility for the individual, P3P protocols must be supported “by the infrastructure.”

Finally, it should be noted that anonymizing proxy servers or networks, which allow individuals to surf or communicate anonymously, pseudonymously, or in an otherwise untraceable manner, depend critically upon a trusted, enabling infrastructure. There may be some linked component that resides on a user’s computer that is under that person’s control, but the network is itself, the PET, and the user interface is just that – an interface.

**PETs Plus recognize the importance of design and architecture**

Do traditional stand-alone PETs, when built into the “infrastructure” suddenly stop functioning as a PET? In a word: No. For example, password managers, “cookie cutters” and spam filters are often held up as examples of PETs, because they are discrete tools that empower users and minimize the unwanted processing of sensitive data. But when these PETs are integrated into operating systems and browsers, do they necessarily lose their privacy-enhancing qualities? Is there a difference between a stand-alone password manager and the one offered by Firefox or Internet Explorer? Are spam filters that are installed and configured exclusively on one’s home computer or client application any more of a PET than those installed and operating at the internet service provider infrastructure level?
I argue that no, PETs can be one or the other, or both. Either way, it is critically important to recognize that the infrastructure is often an essential component of PETs, and can sometimes even become the entire PET.

**PETs Plus promote user confidence and trust**

The (growing) importance of information architecture design and infrastructure has implications for user empowerment and control. Because the behaviour of infrastructure components is often beyond the direct access and control of individuals, a certain degree of reliance and trust is essential. In the context of networked cloud computing and the exponential creation, use and disclosure of personally identifiable information by more and more actors, this reliance and trust must in turn grow. It does not mean that PETs are becoming less relevant. Quite the opposite: PETs must evolve in tandem, and make possible a new era of privacy confidence and trust... enter PETs Plus.

Take, for example, enterprise PETs or corporate PETs, meeting both the needs of the organization and protecting privacy. These are privacy-enhancing technologies that are deployed entirely within information architectures and systems owned and operated by organizations, rather than by individuals. “Enterprise” PETs can facilitate better organizational controls and privacy compliance for all uses of personal data, in a given system. The privacy practices of data minimization and improved security may be fully operationalized but, in place of individual participation, there is a growing focus on ensuring system transparency, consistency, and accountability. One example would be an enterprise privacy technology that attaches privacy policies directly to personal data and automatically tracks their usage, enforcing those policies across the entire enterprise, and beyond.

At this point, while the degree of user participation may diminish, privacy does not. It only takes a short step to recognize that PETs may be built directly into organizational infrastructures in such a way that privacy benefits may be achieved with minimal or no user participation.

In summary, these are examples of PETs Plus – when enterprises or “architectural” PETs achieve both privacy and enterprise functions in a positive-sum way, enabling privacy and system functionality.

---

2 How that trust is secured can vary enormously, e.g., open-source code, open competition and availability of alternatives, third-party testing and certification, warranties and guarantees, reputation, direct audit tools, etc. Indeed, one emerging class of PETs identified is transparency and audit tools that allow individuals to make better informed privacy decisions in their online and offline interactions.
Transformative Technologies

It gets even better: when PETs Plus are applied to traditionally privacy-invasive technologies, such as video surveillance systems – without any meaningful loss of functionality – these technologies can, in effect, be transformed into behaving like privacy-protective ones. This set of PETs Plus we call Transformative Technologies.

I have identified Transformative Technologies in the following traditionally “privacy-invasive” areas:

- Biometrics
- Radio-Frequency Identifiers (RFID)
- Video surveillance cameras
- Network tracing and monitoring
- Whole body imaging
- Online digital identities

Conclusion

PETs Plus are Privacy-Enhancing Technologies applied within a positive-sum, not zero-sum paradigm, often resulting in the creation of Transformative Technologies.

From a privacy perspective, all ICTs are essentially neutral. What matters are the choices made in their design and use – technologies may be designed to be privacy-invasive or privacy-enhancing. PETs embody fundamental privacy principles by minimizing personal data use, maximizing data security, and empowering individuals. The concept of Privacy by Design that I introduced in the ’90s extended the concept of PETs to emphasize the need to embed privacy at the design stages of information technologies, architectures, and systems – all of which are often beyond the control of the individual. Organizations that embed privacy early on will benefit in a number of sustainable ways from the resulting privacy payoff.

Today, these messages are more relevant than ever, as we collectively face a world of ubiquitous data availability (in the words of Professor Fred Cate). Building upon my positive-sum approach to advancing privacy, I encourage the development of a new generation of PETs – PETs Plus – which can actually transform otherwise privacy-invasive technologies into privacy-protective ones, with little or no loss of functionality. This new breed of Transformative Technologies can also transform privacy problems into lasting privacy solutions – ensuring that privacy lives well into the future.
Transformative Technologies Deliver Both Security and Privacy: Think Positive-Sum, Not Zero-Sum
Transformative Technologies Deliver Both Security and Privacy: Think Positive-Sum, Not Zero-Sum

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 user-subjects 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:
Privacy by Design

- 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 of 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,” 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.
Privacy and Video Surveillance in Mass Transit Systems:
A Special Investigation Report

March 2008
Introduction

The significant growth of video surveillance cameras throughout the world, especially as witnessed in the United Kingdom, has created considerable concerns with respect to privacy. This Report was prompted by a complaint received from Privacy International regarding the Canadian expansion of the use of video surveillance cameras in the City of Toronto’s mass transit system. In light of the divergent points of view on video surveillance, in addition to investigating this complaint, my office decided to expand our Report to include a review of the literature, as well as an examination of the role that privacy-enhancing technologies can play in mitigating the privacy-invasive nature of video surveillance cameras. As such, this Report is longer than most, attempting to provide a comprehensive analysis examining the broader context of video surveillance. Given the enormous public support for the use of video surveillance cameras in mass transit systems and by the law enforcement community, addressing this issue broadly, with a view to seeking a positive-sum paradigm through the use of privacy-enhancing technologies, is our ultimate goal.

Background

On October 24, 2007, the Office of the Information and Privacy Commissioner of Ontario (IPC) received a letter of complaint from an organization relating to the deployment of video surveillance cameras throughout the Toronto Transit Commission’s (TTC) mass transit system in Toronto, Ontario. The organization subsequently publicly identified itself as Privacy International, which is based in the United Kingdom.1

The letter of complaint expressed the view that the TTC’s use of video surveillance cameras contravened the privacy provisions of the Municipal Freedom of Information and Protection of Privacy Act (the Act). In their letter, Privacy International argued that the collection principles of the Act “are not being sufficiently attended to in that the collection is not necessary, that the scheme is being deployed without consideration to privacy and associated protocols, and with insufficient consideration regarding access powers.” It argued that the program has been undertaken on the basis of crime prevention and crime detection despite the fact that there is no evidence that video surveillance on public transit systems significantly reduces the level of crime or the

1 The letter of complaint has been posted to Privacy International’s website: http://www.privacyinternational.org/issues/compliance/complaint_ttc_privacy.pdf
threat of terrorist attacks. It also argued that studies indicate that video surveillance has a marginal impact on investigations and that video surveillance cameras are plagued with technological and management issues. Finally, Privacy International stated that the TTC had failed to respect legal requirements for public consultation, disclosure and establishment of a public interest case for its video surveillance system. In order to address these issues, this privacy complaint file was opened (MC07-68), and an investigation commenced.

Before outlining the investigation of this complaint, I will first provide background information on the privacy implications of video surveillance cameras and the manner in which these issues have been addressed by my office over the years. I will also include a discussion of the research on the effectiveness of video surveillance, since this is a pivotal issue in this investigation. For those who may only be interested in the investigation itself, please proceed directly to that part of the report dealing with the specifics of the investigation, beginning on page 74.

Privacy and Video Surveillance

Historically, pervasive video surveillance has posed a threat to privacy and constitutional rights. When controlled by government departments, video surveillance can provide the government with massive amounts of personal information about the activities of law-abiding citizens, going about their daily lives. When individuals know they are being watched, this may have a chilling effect on their freedom to speak, act and associate with others. Since individuals may censor their own activities when they are aware of being watched, video surveillance may also be perceived as a means of enforcing social conformity.

Privacy and the right of individuals to go about their daily activities in an anonymous fashion not only protects freedom of expression and association, but also protects individuals from intrusions into their daily lives by the government. Accordingly, when government organizations wish to use surveillance technology in a manner that will impact the privacy of all citizens, there must be clear justification for doing so. Specifically, the benefits of the technology should justify any invasion of privacy.

It has been argued that individuals cannot have a reasonable expectation of privacy in public places, especially in the case of urban mass transit systems where large volumes of people may be concentrated in relatively restricted spaces. In addition, it has been argued that video surveillance in such places is an enhancement of a person’s natural ability to observe what is happening in public. While the expectation of privacy in public spaces may be lower than in private spaces, it is not entirely eliminated. People do have a right to expect the following: that their personal information will only be collected for legitimate, limited and specific
purposes; that the collection of their personal information will be limited to the minimum necessary for the specified purposes; and that their personal information will only be used and disclosed for the specified purposes. These general principles should apply to all video surveillance systems.

In order to address situations where government organizations elect to deploy video surveillance systems, my office issued Guidelines for the Use of Video Surveillance Cameras in Public Places (the Guidelines), in 2001. These Guidelines were later updated in 2007,2 and are based on the provisions of Ontario’s Freedom of Information and Protection of Privacy Act and its municipal counterpart, the Municipal Freedom of Information and Protection of Privacy Act (the Acts). Since they were issued, the Guidelines have been used by many government organizations to develop and implement video surveillance programs in a privacy-protective manner, in compliance with the Acts.

The Guidelines are intended to assist organizations in determining whether the collection of personal information by means of video surveillance is lawful and justifiable as a policy choice, and if so, how privacy-protective measures may be built into the system. The Guidelines do not apply to covert surveillance, or surveillance when used as a case-specific investigation tool for law enforcement purposes, where there is statutory authority and/or the authority of a search warrant to conduct the surveillance.

Before deciding whether to use video surveillance, the Guidelines recommend that organizations consider the following:

- A video surveillance system should only be adopted after other measures to protect public safety or to deter, detect, or assist in the investigation of criminal activity have been considered and rejected as unworkable. Video surveillance should only be used where conventional means (e.g., foot patrols) for achieving the same law enforcement or public safety objectives are substantially less effective than surveillance or are not feasible, and the benefits of surveillance substantially outweigh the reduction of privacy inherent in collecting personal information using a video surveillance system.

- The use of video surveillance cameras should be justified on the basis of verifiable, specific reports of incidents of crime or significant safety concerns.

- An assessment should be made of the effects that the proposed video surveillance system may have on personal privacy and the ways in which any adverse effects may be mitigated.

2 These Guidelines are available online: http://www.ipc.on.ca/images/Resources/up-3video_e_sep07.pdf
Consultations should be conducted with relevant stakeholders as to the necessity of the proposed video surveillance program and its acceptability to the public.

Organizations should ensure that the proposed design and operation of the video surveillance system minimizes privacy intrusion to that which is absolutely necessary to achieve its required, lawful goals.

Once a decision has been made to deploy video surveillance, the Guidelines set out the manner in which video surveillance cameras should be implemented in order to minimize their impact on privacy.

I have taken these Guidelines into consideration in investigating the TTC’s video surveillance program.

Evidence of the Effectiveness of Video Surveillance

In its letter of complaint, Privacy International made reference to empirical studies addressing the efficacy of video surveillance. Since there is considerable disparity in the views relating to its efficacy, my office decided to conduct a selective review of the literature on the effectiveness of video surveillance on potential offenders and on criminal justice processes and outcomes. The focus of the review was on research conducted over the past 10 years.

The literature review found numerous studies on the effectiveness of video surveillance on crime, in a broad range of settings. These studies varied substantially, however, in terms of their methodological rigour. Since an in-depth review of each of these studies was not feasible within the course of our investigation, we decided to rely on the work of credible experts who evaluated a broad range of studies on the topic and drew their conclusions on the basis of the quality of the empirical evidence before them.

There are significant challenges to conducting high-quality research on video surveillance in natural settings because of the difficulty of controlling the multitude of extraneous factors that may influence the research outcomes. In order to demonstrate the effectiveness of video surveillance on crime prevention, a study would have to show either a decrease in the rate of crime, or a slowing in an increasing crime rate in locations where video surveillance cameras had been implemented. To confirm that any such change was attributable to video surveillance, a study would have to show that a similar decrease in crime or a slowing in the increasing crime rate did not occur in comparable locations where video surveillance cameras had not been implemented (control areas). In addition, in order to confirm that such changes in crime rates were long-term as opposed to transient, the evaluation
period would have to extend for a substantial period of time. Unfortunately, research with this level of methodological rigour is extremely rare.

In 1997, California-based Marcus Nieto examined whether the use of video surveillance in public and private places was effective in preventing crime and concluded that the data suggested that the technology was successful in both reducing and preventing crimes, and was helpful in prosecuting individuals caught in the act of committing a crime.\(^3\) Nieto looked at evaluations of the technology from around the world.

In 2001, in its *Final Report: Evaluation of the NSW Government Policy Statement and Guidelines for Closed Circuit Television (CCTV) in Public Places*, the Interdepartmental Committee on video surveillance reported on an evaluation of video surveillance technology throughout New South Wales, Australia.\(^4\) The committee concluded that the anecdotal reports and statistics provided an indication that video surveillance may be effective in certain contexts and had received a high level of support. However, the committee noted that none of the assessments could be viewed as systematic evaluations of the technology.

In 2003, the Royal Canadian Mounted Police commissioned an evaluation of the effects of video surveillance systems on crime.\(^5\) Wade Deisman, Professor of Criminology and Director of the multidisciplinary National Security Working Group at the University of Ottawa, conducted the evaluation. The review showed that “the effects of video surveillance on crime are quite variable and fairly unpredictable”\(^6\) and that the deterrent value of video surveillance varies over time and across crime categories. Video surveillance systems were found to have the least effect on public disorder offences.\(^7\) The magnitude of the deterring effects of video surveillance on crime was found to depend on the location, with the greatest benefit being in parking lots. The evaluation also found that video surveillance cameras did not need to be operational in order to deter crime. The deterring effects were highest when video surveillance was used in conjunction with other crime reduction measures and when tailored to the local setting. Continuing publicity was also required to maintain the positive effects of video surveillance systems on

---


\(^6\) Ibid, page 2.

\(^7\) Public disorder offences may include acts of violence and/or intimidation by individuals or groups of individuals, such as rioting and drunkenness.
crime, over time. No evidence was found of increased conviction rates with the implementation of video surveillance.

In 2002, the Home Office in the United Kingdom issued a report entitled, Crime Prevention Effects of Closed Circuit Television: A Systematic Review. The report was written by Brandon Welsh, Professor in the Department of Criminal Justice at the University of Massachusetts Lowell, and David Farrington, Professor of Psychological Criminology in the Institute of Criminology at the University of Cambridge. The authors assessed 46 relevant studies from both the United States and Britain according to strict methodological criteria and found that only 22 studies were rigorous enough to include in their analysis. On the basis of these 22 studies, they concluded that video surveillance reduced crime to a small degree and was most effective at reducing vehicle crime in parking lots. Video surveillance was found to have little or no effect on crime in public transport and city centre settings.

In 2005, the Home Office in the United Kingdom issued another report on a study of the effectiveness of video surveillance systems. Martin Gill, Professor of Criminology at the University of Leicester, directed the evaluation. The report provides a systematic evaluation of 13 video surveillance projects implemented in a range of contexts, including town centres, city centres, parking lots, hospitals and residential areas. The results were contradictory – crime went down in some target areas while it went up in others. Video surveillance systems installed in mixed category areas (e.g., parking lots, a hospital, etc.) showed the greatest reduction in crime, particularly in parking lots. Impulsive crimes, such as alcohol-related ones, were found to be less likely to be reduced than premeditated crimes, such as auto theft. Violence tended to increase while auto theft tended to decrease, in accordance with trends in national crime statistics.

It is important to note that regardless of the inconclusiveness of the empirical research on the effectiveness of video surveillance, the Home Office in the United Kingdom has not been deterred from supporting the use of this technology. A report issued in October 2007 entitled National CCTV Strategy stated that video surveillance plays a significant role in protecting the public and assisting the police in the investigation of crime.

---

aspects of criminality, including serious crimes and terrorist incidents. The report noted that the contribution that video surveillance has made to the protection of the public and assisting the police in investigating crime has been realized despite the fact that the technology has been “developed in a piecemeal fashion with little strategic direction, control or regulation.” The report recommended the development of a strategy to maximize the potential of the video surveillance infrastructure.

In 2006, the United States Department of Justice, Office of Community Oriented Policing Services issued a report entitled Video Surveillance of Public Places. The report was written by Jerry Ratcliffe, Professor in the Department of Criminal Justice at Temple University. The report provides an overview of video surveillance systems, explores the benefits and problems associated with the technology, and summarizes the findings of numerous evaluations.

The report notes that while there is a general perception among system managers and the public that video surveillance cameras are effective in preventing crime, actual evidence of crime reduction is more difficult to find. Nevertheless, based on the evidence provided by several evaluation reviews, the general findings were as follows:

- Video surveillance is more effective at reducing property crime than violent or public order crime (although there have been some successes in this area);
- Video surveillance appears to work best in small, well-defined areas (such as public parking lots);
- The individual context and the way the system is used appear to be important;
- Achieving statistically significant reductions in crime is difficult due to normal fluctuations in crime rates;
- The involvement of the police is an important determinant of the success of a system; and
- There is an investigative benefit to video surveillance once an offence has been committed.

In summary, the author concluded that, “it is possible to say there was some evidence of crime reduction in most of the systems ... there is a growing list of evaluations that suggest CCTV has had some qualified successes in reducing crime.”

11 Ibid, page 5.
Discussion of the Empirical Research on Video Surveillance

It should be noted that applications of video surveillance vary widely in many aspects. This makes it difficult to make comparisons across studies and to draw general conclusions from the evaluations. For example, applications vary in terms of the following:

- the goals of the applications;
- types of video surveillance technology used;
- passive versus active monitoring of videos;
- types of target areas (e.g., closed versus open);
- size of the target areas;
- density of cameras;
- fixed versus redeployable cameras; and
- involvement of law enforcement.

In addition, while the empirical evidence in support of the effectiveness of video surveillance in combating crime is weaker than might be expected, it is important to note that most of the research has been carried out in the United Kingdom, where video surveillance technology has proliferated, in part, due to substantial amounts of federal government funding. In contrast, the introduction of video surveillance cameras in Ontario has been more selective as it has not yet received large-scale funding from either the federal or provincial governments. Since research shows that situational factors influence the effectiveness of video surveillance cameras, the research findings from other jurisdictions, such as the United Kingdom, may not be directly applicable in the Ontario context.

For example, while video surveillance systems have shown little effect on crime in town centres and city centres in the United Kingdom, a study of the effectiveness of video surveillance cameras on crime in Sudbury, Ontario, showed very positive results.¹⁴ Specifically, the study found that after the first camera was installed, crime rates in the downtown area dropped dramatically. It was estimated that between 300 and 500 robberies, assaults, thefts and other criminal offences have been deterred by the video surveillance project, saving as much as $800,000 in direct monetary losses. In addition, arrests relating to prostitution and drug offences increased by an average of 18 per cent per year, as a direct result of enhanced capacity to detect these crimes. The authors concluded that the video surveillance system had been effective in both deterring and detecting crime.

The discrepancy between the findings in the United Kingdom and those in Ontario could be due to situational variations in the application of the technology. For example, one could speculate that video surveillance systems may be deployed in a more strategic manner in locations where funding for such initiatives is scarce. This may result in greater reductions in local crime rates in such locations when compared to locations where funding is more abundant.

It is also important to note that the research on the effectiveness of video surveillance has been plagued by methodological flaws, most notably the following:

- Lack of suitable control areas (i.e., areas where crime rates have not been influenced by the implementation of other crime prevention measures during the study period);
- Lack of adequate crime statistics (e.g., statistics may not be isolated to the targeted area);
- Crime rates may not be reliable indicators due to changes in the definitions of crimes and changes in the way crimes are reported over time (i.e., individuals may be less inclined to report crimes if they believe there are video surveillance cameras in the area or individuals may be more inclined to report crimes if they believe the police will be able to apprehend criminals due to the availability of video surveillance images that may be used as evidence);
- No assessment of displacement or diffusion of benefits into surrounding areas;
- Inadequate pre- and post-video surveillance time periods in which data are collected;
- The fact that video surveillance may actually increase the detection of certain types of crimes, thereby driving reported crime rates up;
- Many evaluations involved dated video surveillance technology that may be less useful for identifying offenders in comparison to the newer video surveillance technology;
- Video surveillance is seldom implemented in isolation – it is usually implemented as one component of a package of crime prevention measures and therefore its effects are difficult to isolate;
- Cameras are sometimes located in target areas with crime rates that are too low to notice a difference following the implementation of video surveillance cameras;
- Video surveillance cameras are often implemented in a piecemeal manner, making it difficult to compare crime statistics before and after implementation;
Crime rates vary naturally over time and show evidence of seasonality and long- and short-term trends, making it difficult to isolate the effects of video surveillance cameras and making it difficult to obtain statistically significant results;

- Lack of clear objectives for implementing video surveillance cameras, making it difficult to find suitable effectiveness measures;

- Offenders may not be aware of the presence of cameras, making it virtually impossible to deter crime; and

- Very little of the research has been conducted by independent third parties.

Unfortunately, there are no clear conclusions to be drawn. There are substantial challenges in finding statistically significant evidence that video surveillance reduces crime and aids in criminal justice processes. However, it is equally difficult to conclude from the ambiguous findings reported in the literature that video surveillance is not, in fact, effective in deterring criminal activity. This conclusion is supported by other evidence on the effectiveness of video surveillance, particularly in the detection and investigation of crime, which is clearly much less equivocal than the research on the effects of video surveillance in deterring crime.

For example, in 1993, video surveillance images of toddler Jamie Bulger being led away from a Merseyside shopping mall by his two 10-year-old abductors assisted the police in identifying and apprehending his murderers. Video surveillance footage released to the public led to early identification of suspects and played an important role in their subsequent prosecution in the case of the Brixton nail bomber in 1999 and in the failed bombing of London’s subway system on July 21, 2005. In the later case, four men were found guilty of conspiracy for murder for their involvement. More recently, images collected from video surveillance cameras located in a hospital in Sudbury, Ontario, were highly instrumental in identifying and locating a woman who pleaded guilty to having kidnapped a newborn infant from the hospital. Images collected from the camera were very helpful in the return of the infant to his family.

The efficiency with which video surveillance footage has been used in the investigation of terrorism in London dramatically altered perceptions about video surveillance. For example, Nigel Brew, in a research note entitled *An Overview of the Effectiveness of Close Circuit Television (CCTV) Surveillance*, prepared for the government of

15 See the article by Shirley Lynn Scott, “The Video Tape” at the Crime Library website online: http://www.crimelibrary.com/notorious_murders/young/bulger/4.html


Australia in 2005, concluded that “video surveillance may be of more value as a source of evidence than as a deterrent.”18 However, as argued by Michael Greenberger, Director of the University of Maryland Centre for Health and Homeland Security, following the terrorist attacks in 2005, the “effective investigatory use of CCTV is very likely to be a significant deterrence to future terrorist activities on London mass transit.”19

Conclusions from the Empirical Research on Video Surveillance

Since the bulk of the empirical research is deficient in a number of respects, it is difficult to draw any definitive conclusions about the effectiveness of video surveillance cameras. Without an ability to control the many factors that influence outcomes and the context and mechanisms that produce these outcomes, it is not surprising that the results of earlier evaluations have been mixed, conflicting and, at times, contradictory. Video surveillance systems do not appear to have uniform effects across a wide range of crime categories. At present, it is difficult to find unequivocal evidence that video surveillance deters or prevents crime. However, it is equally difficult to conclude the opposite. A more valuable role for video surveillance may be as a source of evidence in the detection and investigation of crime. A much larger body of research, with a consistent degree of methodological rigour, is needed before definitive statements may be made.

Why Video Surveillance Is Believed to Enhance Public Safety

Historically, video surveillance was most often implemented in public spaces because of an expectation of crime deterrence.20 In general, the goal of deterrence and crime prevention strategies is to put in place practices or conditions that will lead potential offenders to refrain from engaging in criminal activities, delay criminal actions, or avoid a particular target. As is the case with many crime prevention strategies, video surveillance aims to make the potential offender believe that there is an increased risk of apprehension. To increase the perception of risk, the potential offender must be aware of the presence of the cameras and believe that

the cameras present sufficient risk of capture to outweigh the rewards of the intended crime. Awareness of the cameras may be enhanced through public education, clear signage, and media coverage of incidents caught on camera. In addition to awareness, however, understanding the consequences of being caught by the cameras requires rational thought. It is unlikely that potential offenders under the influence of drugs or alcohol would be deterred from acts of violence or public disorder by the presence of cameras.

Video surveillance is also believed to reduce crime by helping in the detection, arrest and prosecution of offenders. When an incident occurs in the presence of video surveillance cameras, the police can respond quickly and in a manner that is more appropriate to the situation. To the extent that offenders are captured and convicted using video surveillance evidence, this may prevent them from committing further crimes.

While video surveillance has contributed to the apprehension of criminals in a number of high-profile cases, historically its value has stemmed from its potential to deter rather than detect criminal activity. This view is now changing. The value in detecting crimes is now being considered as a primary goal of video surveillance.

Video surveillance images may also assist the police in investigating crimes. It is important to note that video surveillance footage may not only help the police identify offenders, but may also help in the identification of potential witnesses who may otherwise be reluctant to come forward.

In addition, video surveillance is believed to make people feel more safe and secure. This is an important goal of security programs for all mass transit systems. If members of the public do not feel secure, they may avoid using public transit, thereby decreasing ridership.

In short, there are reasons other than deterrence, as to why video surveillance may help to prevent crime and aid the police in criminal investigations. This may help to explain why video surveillance systems are strongly supported and continue to proliferate.

**Emerging Privacy-Enhancing Video Surveillance Technology**

While technology is essentially privacy neutral, if deployed without careful consideration to its impact on privacy, it may be extremely invasive. I have been a strong advocate for harnessing the strengths of technology and putting them in the service of privacy – enlisting the support of technology to enhance, instead of erode, privacy. Privacy-enhancing technologies (PETs) are those information and
communication technologies that incorporate measures to protect privacy by eliminating or reducing the collection, retention, use and disclosure of personal information. This is often referred to as “data minimization” and increasingly represents a vital component of privacy protection.

To avoid the costly and ineffective retrofitting of technology to address privacy issues after they have been implemented, it is essential that privacy protections be built directly into their design and implementation, right from the outset. This view is captured in my mantra of “privacy by design.” It is incumbent upon those who wish to deploy surveillance systems to be aware of and adopt PETs whenever possible, especially as they become commercially available.

Recent research has shown that it is possible to design surveillance systems in a manner that may successfully address issues of public safety while, at the same time, protecting the privacy of law-abiding citizens.

There are a variety of technologies based on digital image processing that are currently being researched and developed for protecting the privacy of individuals appearing in video surveillance footage. As described in the research literature, these approaches are operating as follows:

Step 1: object detection and segmentation methods for locating objects of interest, such as human faces, within images and video frames; and

Step 2: object obscuration or securing methods, which, after the completion of step 1, manipulate the pixel data so that some or all viewers of the surveillance footage are unable to discern the private object content (which one is seeking to protect from viewing).

For the first step, object detection and segmentation, there are many well-established approaches using pattern recognition algorithms, some of which are currently used in surveillance and recognition systems. For the second step, object obscuration or securing, there are various approaches, the choice of which is dependent upon the application requirements. The simplest approach is to blur or discard (i.e., obscure with a black box) the private object content. The significant limitation of this approach is that the content is irretrievable for future investigative purposes if it is applied immediately during acquisition of the surveillance footage. What is needed is a novel privacy-enhancing approach that allows the personally identifiable information or objects of interest in the original video stream to be securely protected from viewing while, at the same time, preserving the original content stream and enabling this information to be retrieved at a later date, if required.
Innovative Privacy-Enhancing Approach

I am delighted to report that at the University of Toronto, Karl Martin and Kostas Plataniotis have developed such a 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.\(^2\) 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 may 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, the objects of interest could not be decrypted; Figure (c): example where only the texture of the whole body (or only a face for example) is encrypted.](image-url)

---


\(^2\) The figure contains a photograph of one of the researchers. The researcher in the photograph consented to its publication in this Report.
The Pitfalls of a Zero-Sum Approach

Over the years, I have argued that adopting a zero-sum paradigm, where one party wins and one party loses, is ultimately shortsighted and least effective. As a result, my office has developed “positive-sum” models for consideration in the use of emerging technologies, whereby both parties may “win” and neither party must, by necessity, lose. In the scenario involving video surveillance cameras, the police may have a legitimate goal in using video surveillance cameras as a tool in the detection of criminal activity, while, at the same time, individuals have a legitimate expectation that their daily activities will not be monitored and preserved on tape. The innovative work of Martin and Plataniotis provides an ideal example of a positive-sum technology, where both interests can prevail: Video surveillance cameras may be deployed for reasons consistent with public safety and law enforcement; however, no personal information from camera footage is accessible to unauthorized parties not in possession of the decryption key. Strong policies would need to be implemented in conjunction with this technology to restrict access to the decryption key to a limited number of authorized individuals. Protocols should also be developed governing the conditions under which video surveillance footage could be decrypted – for example, only after a crime had been committed or a safety mishap had occurred.

The use of this type of privacy-enhancing technology would thus allow for video surveillance to be conducted without the usual concerns associated with this type of surveillance. For the great majority of the surveillance footage, there would be absolutely no access or viewing of any personally identifiable information, and no unauthorized activities, such as viewing out of curiosity or “leering,” would be possible.23 Therefore, this privacy-enhancing technology would enable both the use of video surveillance cameras and privacy to co-exist, side by side – without forfeiting one for the other: positive-sum, not zero-sum.

23 See Jeffrey Rosen’s seminal book “The Naked Crowd” (2004) for examples of video surveillance voyeurism where unsupervised video surveillance camera operators in the United Kingdom entertained themselves by zooming in on attractive women or couples engaged in sexual activities. In this book, he argues that it is possible to strike an effective balance between liberty and security by adopting well-designed laws and technologies.
Conduct of the Investigation

As discussed above, in its letter of complaint to the IPC, Privacy International raised concerns regarding the TTC’s deployment of video surveillance cameras and asserted that the TTC’s use of video surveillance was not in accordance with the privacy provisions of the Act. Privacy International’s letter made reference to past studies on the efficacy of video surveillance, technological concerns regarding the use of video surveillance, as well as legal considerations.

In order to provide the TTC with the opportunity to respond to the issues raised in the complaint, my office met with their staff. I also wrote to the TTC to confirm my understanding of the background facts pertaining to this complaint and to obtain the TTC’s written representations on whether the operation of the video surveillance system was in accordance with the provisions of the Act. The TTC provided a thorough and detailed response. Privacy International was also provided with an opportunity to submit additional information, but declined to do so.

Staff from my office also conducted a site visit to examine the video surveillance system in place at a representative TTC subway station.

Extent of Surveillance

The TTC indicated that there are currently cameras in both the TTC’s subway system and on its surface vehicles (which comprise buses and streetcars). With respect to the TTC’s fleet of 1,750 surface vehicles, 286 buses are fully equipped with four cameras on each bus, for a total of 1,144 cameras. (To date, no cameras have been installed on streetcars.) With respect to the TTC’s subway system, there are currently 1,200 cameras located throughout the 69 stations. These cameras are generally located at choke points (major access points), Designated Waiting Areas, automatic entrances, elevators, collector booths, and other site-specific areas of concern.

The TTC expressed its plans to expand its surveillance program on both surface vehicles and within the subway system. Specifically, the TTC plans to equip its remaining 1,464 surface vehicles with cameras so that all surface vehicles will have cameras by the end of 2008. With four cameras planned for each vehicle, this would amount to a total of 7,000 cameras on the TTC’s entire fleet of surface vehicles. In addition, there are plans to install five cameras per vehicle on all 144 Wheel Trans vehicles (a total of 720 cameras) by the end of 2008. With respect to the subway system, the TTC plans to increase the number of cameras on the subway system by 1,100, from the current number of 1,200, to a total of 2,300 by the end of 2011. In addition, the TTC plans to introduce cameras inside subway cars. Currently, there are plans to install a total of 1,014 cameras on 39 new subway train sets that will begin to be introduced into the TTC system in late 2009.
It is our understanding that all of the existing and proposed cameras are or will be located in places where they have the potential to capture images of individuals.

**Operation of the System**

The TTC has also provided background information on the operation of the cameras. Specifically, the TTC has provided information about the retention of video surveillance images; the type of technology used; the monitoring of live video surveillance images; and access to recorded video surveillance images on both surface vehicles and within the subway system.

With respect to retention schedules, the TTC explained that recorded video surveillance images from surface vehicles are retained for a period of 15 hours, at which time they are automatically overwritten. For the cameras operating in subway stations, the recorded video surveillance images are retained for a maximum period of up to seven days, at which time they are automatically overwritten.

With respect to the type of video surveillance technology used, the TTC indicated that the cameras located on surface vehicles all utilize digital technology. The cameras currently located within the subway system utilize both analog and digital technology.

With respect to the active monitoring of the video surveillance images, the TTC stated that the cameras located on surface vehicles are not monitored nor are the images accessible by the vehicle drivers. The only way that video surveillance images from surface vehicles could be actively monitored from a remote location would be through a wireless video surveillance network. Such a network has not been installed by the TTC. With respect to the subway system, the TTC noted that, while these cameras are not generally monitored, cameras from 16 subway stations are currently linked through a fibre-optic cable that permits live remote access to video surveillance images by four departments of the TTC: Transit Control, Signals/Electrical/Communications Maintenance Department, Signals/Electrical/Communications Engineering Department, and Special Constable Services. The purposes for which each of these departments may access the live video surveillance images is described below.

With respect to Transit Control, although the live feed and monitors are "on" 24 hours a day in case a problem arises within the subway system, the video surveillance images are not actively monitored. Transit Control determines which subway platforms are monitored through the live feed. Approximately eight cameras can be displayed at one time. With respect to both Signals/Electrical/Communications Engineering and Maintenance Departments, the cameras are not actively monitored. Remote access to the video surveillance signals is used strictly for maintenance-related issues, such as system failure, camera failure, network failure or preventative maintenance. Special Constable Services also do not actively monitor the live video surveillance feed. All access is strictly logged and incident driven.
In addition to the live video surveillance feed from cameras linked to the fibre-optic cable, there is a live feed to monitors that are viewable by a TTC Superintendent on weekdays during the morning and evening rush hours. The live feed monitors the subway platforms at crossover stations, where the north-south subway line meets the east-west subway line. The live video surveillance images are used strictly for the purpose of monitoring overcrowding on the platforms to ensure passenger safety. If necessary, public announcements are made by the Superintendent to provide updates or directions to passengers.

Currently, with respect to access to recorded video surveillance images, from both surface vehicles and the subway system, when an incident has taken place, an investigator must isolate and copy the images prior to the expiration of the retention period in order to use them during the course of an investigation. The ability to access and download recorded video surveillance images is therefore strictly controlled. Investigations may be conducted internally by the TTC, or by an external law enforcement agency, such as the Toronto Police Services.

In addition, once a Memorandum of Understanding (MOU) is signed between the Toronto Police Services Board and the TTC, the Police will have direct remote access to the recorded video surveillance images collected in the subway system. All access to the video surveillance images will be incident driven and require a case file number. Access will be limited to eight individuals within the Video Services Unit. All access will be fully logged.

The TTC’s operation of the video cameras is governed by its “Video Recording Policy” (the Policy), which has been provided to my office in draft form. The Policy is not yet complete and has not been officially adopted by the TTC. Once in force, the Policy will address all major aspects of the TTC’s usage of their cameras, including:

- a statement of the program’s rationale and objectives;
- the responsibilities of various job designations within the TTC regarding the surveillance system;
- the requirement that Notice of Collection be provided to all TTC passengers whose images are collected through the surveillance cameras;
- procedures for responding to a potential privacy breach; and
- acceptable retention periods for recorded images.

Public Consultation
The TTC stated that it has engaged in various forms of public consultation on video surveillance at different points in time. For instance, with respect to cameras within the subway system, during the design of the Sheppard Subway Extension, a Personal Security Design Review Group (PSDRG) was created in order to provide input into security features of the new subway line, including the installation of cameras. The TTC stated that the PSDRG was comprised of various public interest
groups, including the Toronto Safe City Committee and the Metro Action Committee on Public Violence against Women.

With respect to the use of video surveillance cameras in new subway cars, the TTC stated that it had conducted a public viewing of a mock-up of the new subway car from June 6 to July 21, 2006, and had invited the public to comment on its features, including the use of video surveillance cameras.

For the cameras planned on streetcars, the TTC also noted that it has been involved in a public consultation with respect to the purchase of new streetcars. Among other things, this public consultation dealt with the potential installation of video surveillance cameras. In addition, the TTC stated that recommendations relating to the purchase of additional cameras for surface vehicles have been the subject of public reports, and that any group wishing to provide feedback on such reports would have the option of doing so at a TTC Commission meeting.

**Issues Arising in the Investigation**

I have identified the following issues arising from this investigation, each of which will be discussed in turn.

(A) Is the information collected by the TTC’s video surveillance cameras “personal information” as defined under section 2(1) of the Act?

(B) Is the collection of personal information by the TTC’s video surveillance cameras in compliance with section 28(2) of the Act?

(C) Is the Notice of Collection provided to passengers in compliance with section 29(2) of the Act?

(D) Is the disclosure of personal information to the Toronto Police Services in compliance with section 32 of the Act?

(E) Does the TTC have adequate security measures in place to safeguard the personal information collected?

(F) Does the TTC have proper destruction processes in place for recorded information that is no longer in use?

(G) Does the TTC have proper retention periods in place for personal information that is collected?

(H) Has the TTC undertaken all appropriate steps prior to implementing video surveillance?

(I) Is the TTC’s video surveillance system subject to regular audits?

---

24 See the TTC website: [http://www.ttc.ca/postings/gso-comrpt/](http://www.ttc.ca/postings/gso-comrpt/)
Issue A: Is the information collected by the TTC’s video surveillance cameras “personal information” as defined under section 2(1) of the Act?

In order for a given record of personal information to be subject to the privacy provisions of the Act, it must qualify as “personal information” under the definition set out in section 2(1). Section 2(1) of the Act states, in part:

“personal information” means recorded information about an identifiable individual, including,

(a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,

(b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

(c) any identifying number, symbol or other particular assigned to the individual,

(d) the address, telephone number, fingerprints or blood type of the individual,

(e) the personal opinions or views of the individual except if they relate to another individual,

(f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,

(g) the views or opinions of another individual about the individual, and

(h) the individual’s name if it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual; … .

[emphasis added]

The Guidelines state:

Personal information is defined in section 2 of the Acts as recorded information about an identifiable individual, which includes, but is not limited to, information relating to an individual’s race, colour, national or ethnic origin, sex and age. If a video surveillance system displays these characteristics of an identifiable individual or the activities in which he or she is engaged, its contents will be considered “personal information” under the Acts.25

In this case, the records at issue are the images of individuals that are captured by cameras situated within the TTC system. Clearly, such images are capable of identifying particular individuals and therefore, constitute “recorded information about an identifiable individual.”

I am satisfied that the records in question qualify as “personal information” under section 2(1) of the Act. I note that the TTC concurs with this position.

**Conclusion:** The information collected by the TTC’s video surveillance cameras qualifies as “personal information” as defined under section 2(1) of the Act.

**Issue B: Is the collection of personal information by the TTC’s video surveillance cameras in compliance with section 28(2) of the Act?**

In its letter of complaint to the IPC, Privacy International focused on the issue of whether the TTC’s collection of personal information through the video surveillance cameras was permissible under the Act, and stated:

> In this complaint we argue that the collection principles are not being sufficiently attended to in that the collection is not necessary, that the scheme is being deployed without consideration to privacy and associated protocols, and with insufficient consideration regarding access powers.

The section of the Act that addresses the collection of personal information is section 28(2), which establishes a basic prohibition on the collection of personal information, but states that there are three circumstances under which the collection of personal information may take place. Section 28(2) states:

> No person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity.

In order for a particular collection practice to be in accordance with the Act, it must be shown to satisfy at least one of the three conditions set out in section 28(2). In other words, the institution must show that the collection of personal information is either, (1) expressly authorized by statute, (2) used for the purposes of law enforcement, or (3) necessary to the proper administration of a lawfully authorized activity.

The first step in the section 28(2) analysis is to address whether any of the above conditions apply to a given collection of personal information. In this case, the TTC has not provided reference to a statute that provides the express authorization for the collection of personal information through video surveillance. Accordingly, the first condition does not apply.
With respect to the remaining two conditions, in its letter of complaint to the IPC, Privacy International stated that the primary area of focus should be the third condition, which can also be referred to as the “necessity condition.” In its letter, Privacy International made reference to the Ontario Court of Appeal’s decision in *Cash Converters Canada Inc. v. Oshawa (City)*\(^{26}\) (Cash Converters) in stating:

> We understand that this is arguably a law enforcement activity and therefore legal exemptions exist for some data privacy principles, as under s.28(2) of MFIPPA. Recently the Ontario Court of Appeal ruled, in *Cash Converters Canada Inc. v. Oshawa (City)*, that where identifiable information is made available to the police it must first meet the necessity condition “where the institution must show that each item or class of personal information that is to be collected is necessary to properly administer the lawfully authorized activity”. When it is possible to find other ways of achieving the stated lawful goals then the institution must choose another route. We do not believe that the TTC has adequately addressed the necessity of this information collection and has not considered access policies.

While the necessity condition is certainly applicable to this investigation, an additional condition that should be considered is the second condition of 28(2), which permits the collection of personal information that is used for the purposes of law enforcement (the law enforcement condition). In the *Cash Converters* decision, the law enforcement condition was not applicable because the collection of personal information at issue was a collection pursuant to a municipal by-law of the City of Oshawa. Under Ontario’s *Municipal Act*, a municipality is not permitted to enact a by-law for the purpose of law enforcement. Therefore, consideration of the second condition was not an option. That is not the case in the present investigation.

I will now proceed to consider the application of both the necessity condition and the law enforcement condition in section 28(2) of the Act.

**Necessary to the Proper Administration of a Lawfully Authorized Activity (The Necessity Condition)**

In *Cash Converters*, the Ontario Court of Appeal adopted the approach my office has taken in the past with respect to the application of the necessity condition and stated:

> In cases decided by the Commissioner’s office, it has required that in order to meet the necessity condition, the institution must show that each item or class of personal information that is to be collected is necessary to properly administer the lawfully authorized activity. Consequently, where the personal information would merely be helpful to the activity, it is not “necessary” within the meaning of the Act. Similarly, where the
purpose can be accomplished another way, the institution is obliged to choose the other route.27

Based on the test established by my office, and adopted by the Court of Appeal, in order to satisfy the necessity condition, the institution must first identify the “lawfully authorized activity” in question, and second, it must demonstrate how the collection of personal information is “necessary,” not merely helpful, to the achievement of this objective. In addition, this justification must be provided for all classes of personal information that are collected.

In this case, the “activity” in question is the operation of a public transit system by the TTC. The TTC is lawfully authorized to operate under Part XVII of the City of Toronto Act, 2006, which provides that the TTC has the exclusive authority to establish, operate or maintain “a local passenger transportation system within the City.” Therefore, in order to satisfy the necessity condition under section 28(2), the TTC must demonstrate that its collection of personal information through use of video surveillance cameras is necessary to the proper operation of a public transportation system within the City of Toronto.

In considering whether the necessity condition has been satisfied, I have reviewed the documentation provided by the TTC, the information contained in the letter of complaint provided by Privacy International, and the research on the topic discussed earlier in this Report. In addition, during the course of the investigation, my office found additional information pertaining to video surveillance in mass transit systems, which I have also taken into consideration in determining the necessity of the collection. All of this documentation is discussed below.

Video surveillance is not a new phenomenon in mass transit systems. For years, public transit systems in North America have relied on video surveillance cameras to improve their operations and to enhance public safety and security.

It has been widely recognized that safety and security are essential to the proper functioning of mass transportation systems.28 Six relevant goals have been proposed for any mass transit security system:

- Awareness of the risks to employees and users of the system, including the nature, level and impact of each risk;
- Mitigation of each risk to the greatest extent possible and an understanding of the nature of any unmitigated risks;

Awareness of all threats to the proper functioning of the system and mitigating those risks to the greatest extent possible;

Development of appropriate responses to risk events, both during and after such events;

Understanding the perceptions and concerns of employees, users, and potential users of the system; and

Responding to concerns about safety and security through actions and communications.29

Typically, mass transit systems have multiple locations, are distributed over large areas, are complex, and have a high volume of passengers. These features of transit systems conspire to make it extremely difficult to achieve the necessary safety and security goals. Video surveillance is viewed as an essential tool for helping to fulfill some of these security goals. Video surveillance is said to serve a number of key functions within mass transit systems, namely:

Prevention of accidents by monitoring overcrowding, monitoring of individuals in dangerous situations, and monitoring of individuals who may be a danger to themselves;

Organization of the movement of individuals to avoid bottlenecks and to ensure smooth passenger flows;

Prevention of crime, public disorder and terrorist acts by monitoring crowd and individual behaviour, and directing security personnel; and

Assisting in the investigation of incidents by determining how they occurred, identifying potential offenders and witnesses; and providing evidence of criminal or possible terrorist activities.30

With respect to the TTC in particular, the Operator Assault Task Force, consisting of representatives of the TTC and the Amalgamated Transit Union Local 113, was created in 2002 in response to statistics indicating an increase in the number of operator assaults in the Toronto transit system. In 2005, the Task Force issued a report that recommended the implementation of video surveillance cameras on all buses and streetcars to assist in preventing operator assaults.31

On January 28, 2008, a major newspaper, the Toronto Star, reported on an investigation into the impact of work-related stress on TTC bus, streetcar and subway

operators. During the Toronto Star investigation, the reporters obtained information about occupational injury and disease reports filed with the Workplace Safety and Insurance Board, over a five-year period ending in 2005. The investigation, which included interviews with TTC drivers, revealed that at least 181 drivers had filed claims for post-traumatic stress disorder, missing an average of 49 days of work. Post-traumatic stress disorder, associated with the witnessing or experiencing of a traumatic event involving the threat of injury or death, was found to be the second leading cause of lost workdays at the TTC. Drivers were found to have suffered a wide range of abuse on the job – being shot at, spat on, punched, head-butted, slashed with broken bottles, swarmed, kicked and beaten, to name a few examples. The rate of post-traumatic stress disorders among drivers was found to be four times higher than that of Toronto police officers. An additional 102 TTC operators reported missing weeks or months of work due to anxiety, neurotic disorders, and depression. TTC operators were found to report these disorders more often than any other workers in Ontario. The Toronto Star investigation also revealed that the number of reported crimes on TTC property had increased dramatically, from 2,744 in 2005 to 3,415 in 2006 – an increase of 24 per cent.

As part of the critical infrastructure of modern societies, it is generally accepted that mass transit systems are viewed as highly desirable targets for terrorists. Consequently, in addition to dealing with operator assaults and crime at the local level, mass transit systems have found themselves more recently in a position of having to address issues of national security. Accordingly, video surveillance cameras within mass transit systems are being upgraded and expanded to deal with the increased potential of a terrorist threat.

On March 20, 1995, subways in Tokyo, Japan, were the target of a poison gas attack, an act of domestic terrorism perpetrated by members of Aum Shinrikyo. In five coordinated attacks, the perpetrators released sarin gas on several lines of the Tokyo Metro, killing 12 people, severely injuring 50, and causing vision problems for nearly 1,000 others. The attack was directed against trains passing through Kasumigaseki and Nagatacho, home to the Japanese government.

More recent high-profile attacks on public transit systems in Europe underscore this potential terrorist threat. In March 2004, there was a series of coordinated bombings against the commuter train system of Madrid, Spain, killing 191 people and wounding 1,755. On July 7, 2005, there was a series of coordinated terrorist bomb blasts that hit London’s public transport system during the morning rush.

See the Toronto Star, “TTC drivers in crisis: Star investigation finds frequent abuse at work puts them at high risk of stress disorder,” January 21, 2008.

Aum Shinrikyo was a religious organization that turned to terrorist tactics, apparently to hasten the apocalypse.
hour. At 8:50 a.m., three bombs exploded within 50 seconds of each other on three London subway trains. A fourth bomb exploded on a bus nearly an hour later, at 9:47 a.m. in Tavistock Square. The bombings killed 52 commuters and four suicide bombers, injured 700, and caused disruption of the city’s transport system (severely for the first day), as well as immobilizing the country’s mobile telecommunications infrastructure.

With respect to the TTC, in 2004 there were two national security investigations involving activities within the Toronto subway system. At that time, upgrades to the TTC security system were recommended by the Chief of the Toronto Police Services. This recommendation was supported by the Royal Canadian Mounted Police (RCMP) Integrated Security Enforcement Team. In addition, an independent security consultant had recommended the implementation of a system-wide surveillance system for each station and all subway cars following a terrorism-specific risk and vulnerability assessment of the TTC.

The reports, studies and investigations discussed above provide compelling evidence that public safety and security needs on mass transit systems in general, and operator assaults and crime within Toronto’s public transit system in particular, represent a pressing and substantial societal concern. I will now proceed to assess whether video surveillance would, in fact, address this pressing and substantial societal concern.

In May of 2001, prior to the terrorist events on September 11th, the National Center for Transit Research issued a report outlining the results of a survey of transit agencies throughout the United States with respect to the issue of operator assaults and public safety. Of the 32 agencies that responded to the survey, the majority (26) reported having some type of surveillance system in place. Surveillance cameras in public transit systems were found to be implemented for one or more of the following reasons:

- Crime prevention and response
- Risk management
- Response to events in progress
- Customer service
- Employee security and other employee-related issues
- Legal evidence

By far, the great majority of transit agencies that used video surveillance (all but one surveyed) indicated that they would recommend the technology to other agencies. Agencies that responded to questions about the effectiveness of surveillance in reducing incidents of crime, rated their systems as being above average. Many reported measurable reductions in the number of assaults and incidents of vandalism. In response to the question relating to the effectiveness of surveillance in achieving criminal convictions, agencies rated their systems as being somewhat better than average. The majority of agencies also reported increases in both riders’ and operators’ perceptions of security linked to the use of video surveillance.

The TTC conducted a survey of 26 transit agencies in North America regarding the use of video surveillance cameras on transit vehicles. The vast majority of the transit agencies that participated in the survey reported very positive outcomes with video surveillance, including the following: dramatic decreases in crime, reductions in operator and customer assaults, reductions in fraudulent insurance claims, reductions in complaints, improved perceptions of security, the identification, apprehension, and prosecution of suspects in criminal investigations, and the control of student behaviour problems.

In order to determine the use and effectiveness of the existing video surveillance cameras in the Toronto subway system for investigating crimes, the TTC examined requests from law enforcement investigators for information, during the period from January 2007 through July 2007. The study found that 86 per cent of the law enforcement investigators who responded reported that the video images provided positive investigative value. Further, 38 per cent of the respondents indicated that the suspect or suspects caught on camera were successfully apprehended as a result of the images that had been retrieved through the video surveillance cameras.

In the United States, the Department of Homeland Security (DHS) has taken several steps to manage risk and strengthen their nation’s rail and transit systems, including offering grants to state and local governments for programs and equipment to help manage this risk. Training and deploying manpower and assets for high-risk areas, developing and testing new technologies, and performing security assessments of systems across the country are other measures being taken by the department. Similarly, the Canadian government has also allocated funding for transit security that will “improve security for all who use urban transit in Canada.” Video surveillance is viewed as one of the mechanisms of a broader program to address these security issues on mass transit systems.

35 A copy of the report on this evaluation was provided to the IPC in the TTC’s representations.
36 A summary of this research was provided to the IPC in the TTC’s representations.
The United States government’s funding for security programs and state and local government use of these funds for video surveillance programs was the subject of a DHS workshop held on December 17-18, 2007. The department was seeking input into best practices for states that receive funding for video surveillance installations that would assist the government in ensuring the protection of privacy and civil liberties. A broad range of perspectives were represented at the conference, held in Washington, D.C. On one side of the spectrum, civil liberties groups argued that public video surveillance systems threatened privacy, especially when used in combination with other technologies (e.g., data mining, GPS tracking, RFID, Internet, heat sensing video), and have a real potential to change the relationship between the public and the government. On the other side of the debate, law enforcement and emergency management groups noted the need for video surveillance as a key tool to deter criminals; support apprehension and investigation; increase perceptions of safety; promote commerce; and aid in prosecutions.

Interestingly, however, one of the areas in which there was general agreement and acceptance of video surveillance was in the area of mass public transit. The view was that in light of the extensive areas involved (tunnels, platforms, stairways), the high numbers of passengers (especially during rush hours) and the around-the-clock operating hours of the system, the ability to deal with security issues could not feasibly be limited to increasing the number of security personnel. It was widely acknowledged that one or more cameras could easily cover far more territory than one human being. Similarly, there was general agreement that it would be extremely cumbersome (and impractical) to install a screening mechanism like those existing in airports. Consequently, the views of both privacy advocates and those in emergency management and law enforcement converged on the need for video surveillance in urban mass transit systems – all agreed that the use of video surveillance cameras in this context was justifiable.

There was also another use of video surveillance that did not appear to be particularly objectionable to civil libertarians and privacy advocates, namely the use of such surveillance for the purpose of workplace safety. As noted above, workplace safety, particularly with respect to operator assaults, has been a key issue for the TTC.

Consistent with the views expressed above, there is also evidence to suggest that the general public recognizes that video surveillance may be justifiable in certain high-risk locations and that there is a difference between real-time versus archived video surveillance. For example, in one study conducted by Christopher Slobogin,


39 Conclusions based on extensive discussions with Washington conference panelists.
190 people who had been called for jury duty in Gainesville, Florida, were presented with 20 scenarios of video surveillance by the police. The subjects were asked to assume that the target of the surveillance was innocent of any criminal activity. They were then asked to rate the “intrusiveness” of the surveillance on a scale of 1 to 100, with 1 being “not intrusive” and 100 being “very intrusive.” Subjects rated the video surveillance of national monuments and transportation centres, such as airports and train stations, as being minimally invasive (M=20). On average, video surveillance of streets with the tapes destroyed after 96 hours was rated slightly above the middle on the intrusiveness scale (M=53), while street surveillance without the destruction of tapes was rated as being significantly more intrusive (M=73). This supports the position that the public may not view video surveillance in mass transit systems as being unreasonable, especially if the tapes are destroyed within a reasonable time frame. This study is relevant in the context of the present investigation since the TTC does not actively monitor live video surveillance images and recorded video surveillance images are destroyed after a short retention period, unless they are used for an investigation. Thus, the type of video surveillance being undertaken in the Toronto transit system seeks to minimally impact privacy rights, and may not be perceived as being highly invasive by the general public.

The TTC also noted that the use of video surveillance cameras by transit authorities is quite common, not only in Canada, but around the world. With respect to Canada, the TTC provided information demonstrating that the transit authorities in both Montreal and Vancouver are deploying rail-based video surveillance systems that are far broader in scope than what is being planned for the TTC’s subway system.

In its letter of complaint to the IPC, Privacy International stated, with respect to the TTC’s video surveillance system, “that the collection is not necessary, that the scheme is being deployed without consideration to privacy and associated protocols, and with insufficient consideration regarding access powers.” I have considered these claims in light of the materials provided by the TTC in response to this complaint and the other documentation cited in this Report. I will address the issues of privacy protocols and access powers in the latter sections of this Report.

To support its position that the collection of information through video surveillance in the Toronto public transit system is unnecessary and disproportionate, Privacy International has disputed the TTC’s claim that the expanded video surveillance system would reduce the incidence of crime, while also improving counter-terrorism measures. Specifically, Privacy International referred to a report on a pilot


41 The research was summarized in the TTC’s representations to the IPC.
project launched in the Berlin underground. An interim report on the effectiveness of the scheme found that video surveillance did not reduce the incidence of criminality, but rather led to a small increase.

After reviewing an English translation of this study, I noted a number of shortcomings: the time frame for the evaluation of the pilot project was extremely short (i.e., five months); while video surveillance may not have reduced the rate of crime, it was successful in achieving other safety and security objectives, such as documenting attacks on employees. Recall that the objectives of video surveillance in mass transit systems are multifaceted, going beyond finding reductions in crime. Further, the challenges in finding statistically significant reductions in crime rates, in any particular evaluation study, have already been discussed at length earlier in this Report.

Privacy International also pointed to research conducted in the United Kingdom to demonstrate the lack of effectiveness of video surveillance in preventing crime and providing investigatory evidence. While I agree that video surveillance may not be a “silver bullet” in this regard, I again note that there are broader goals for its use in mass transit systems and that, given the massive scope of such systems, there are few viable alternatives. A combination of measures, each with their own recognized limitations, is, in my view (and that of many security experts), the best option for potentially achieving the broad safety and security objectives of mass public transit systems.

Underlying much of the information provided by the TTC is the notion that mass transit systems have specific security requirements that give rise to the need for video surveillance. Since mass public transit often involves the movement of large numbers of passengers in small spaces, the risks to passenger security may be easily distinguished from those in outdoor public spaces.

In addition to security, mass transit systems are also concerned with passenger health and safety, operator safety, and crowd control issues that arise from large numbers of passengers on the system. Accordingly, in considering a threshold to determine whether the use of video surveillance is necessary, I am cognizant of the unique and multifaceted needs of mass transit systems such as the TTC.

The documentation reviewed indicated that there is widespread perception among transit system operators and the general public that video surveillance systems are useful in preventing crime and aiding in criminal justice processes. There is also a growing body of empirical evidence to suggest that video surveillance systems may be an effective part of a crime prevention and national security strategy,

---

42 See the article “Study shows video surveillance on the Berlin underground has not improved safety,” Heise Online, October 10, 2007 available online: http://www.heise.de/english/newsticker/news/97168
aiding in police investigations. In addition, transit system security experts and national security experts continue to strongly recommend the use of video surveillance systems as one component of a comprehensive security strategy for mass transit systems. I have taken all of these factors into consideration in assessing whether or not the TTC has sufficient justification for expanding its use of video surveillance.

In my view, safety and security are essential components to the proper functioning of the Toronto public transit system. In order to preserve the safety and security of the system, the TTC must address not only the growing issues of operator assaults, crime on the TTC, and the potential threat of terrorism, but especially the challenge of moving hundreds of thousands of passengers safely and quickly, on a daily basis. Given the nature of the safety and security needs, and the massive scope and complexity of the public transit system in the City of Toronto, achieving these goals through a combination of other measures (e.g., increased security personnel, enhanced lighting) would not be feasible. The best strategy would be to employ the full range of safety and security options available, which would include video surveillance.

Finally, to return to the test expressed by the Ontario Court of Appeal in Cash Converters, in order for a given collection of personal information to satisfy the necessity condition:

... the institution in question must demonstrate that each item or class of personal information that is to be collected is necessary to properly administer the lawfully authorized activity. Consequently, where the personal information would merely be helpful to the activity, it is not “necessary” within the meaning of the Act.

In this case, the sole class of personal information at issue is the images of individuals that are passengers on the TTC system. Based on the foregoing, I am satisfied that the collection of individuals’ images is not merely helpful, but is also necessary to the proper administration of the TTC. Accordingly, I am satisfied that the collection of personal information through the use of video surveillance cameras meets the necessity condition, and is therefore in compliance with section 28(2) of the Act.

Used for the Purposes of Law Enforcement (Law Enforcement Condition)

Although I have concluded that the TTC’s collection of personal information through video surveillance satisfies the necessity condition (i.e., that it is necessary to the proper administration of a lawfully authorized activity), and is therefore permissible under section 28(2) of the Act, I will now proceed to consider whether the collection would also be upheld under the law enforcement condition (i.e., that it is used for the purposes of law enforcement).
The TTC has stated that the images collected through its video surveillance system are used for the purposes of law enforcement, and has made reference to the activities of staff working in the TTC’s Special Constable Services Department, who are the primary users of the recorded images collected through the surveillance system.

The definition of “law enforcement” is contained in section 2(1) of the Act, which states:

“law enforcement” means,

(a) policing,

(b) investigations or inspections that lead or could lead to proceedings in a court or tribunal if a penalty or sanction could be imposed in those proceedings, or

(c) the conduct of proceedings referred to in clause (b);

With respect to the role of staff working in Special Constables Services Department, the TTC has stated:

… the employees within our Special Constable Services Department have been granted “special constable” status by the Toronto Police Services Board and the Solicitor General. As such, special constables have been conferred the powers of a police officer for specific purposes, including enforcing the Criminal Code throughout the transit system.

The TTC’s description of the powers of a “Special Constable” are supported by section 53 of the Police Services Act, which states, in part:

(1) With the Solicitor General’s approval, a board may appoint a special constable to act for the period, area and purpose that the board considers expedient.

…

(3) The appointment of a special constable may confer on him or her the powers of a police officer, to the extent and for the specific purpose set out in the appointment.

…

In addition to the Police Services Act, further details about the status of TTC Special Constables may be found in a May 9, 1997 Agreement (as amended) between the Toronto Police Services Board (the Board) and the TTC, which sets out the powers, jurisdiction and certain procedures of the TTC Special Constables.
TTC Special Constables may enforce various federal and provincial statutes, including the federal *Criminal Code* and related drug and controlled substances legislation, the provincial *Mental Health Act, Trespass to Property Act, Liquor Licence Act* and specified sections of the *Provincial Offences Act*. In addition, TTC Special Constables may enforce TTC By-Law #1, which sets out the rules that passengers are required to follow to promote, among other goals, public safety and security. For example, the by-law provides that:

No person shall commit any nuisance, disturb the peace, or act contrary to public order, in or upon any vehicle or premises of the Commission.

No person shall carry, nor shall the Commission be required to carry on any vehicle, any goods which are of an offensive, dangerous, toxic, flammable or explosive nature that are likely to alarm, inconvenience, cause discomfort, or injure any person, or cause damage to property, whether or not such goods are contained in an approved container, without authorization.

The jurisdiction of the TTC Special Constables is subject to geographic restriction. TTC Special Constables’ jurisdiction is limited to properties and vehicles under TTC control, and all facilities and leased/rented properties affiliated or associated with the TTC, within the City of Toronto. Additionally, if an offence originates on, or is in relation to, TTC property, a TTC Special Constable may investigate such an offence within the City of Toronto.

The Agreement also sets out procedures relating to the investigative authority in certain situations and with respect to certain offences between the Police and TTC Special Constables. For example, if a Police officer and a TTC Special Constable both attend a call within the geographic jurisdiction of the TTC, or if a dual procedure or indictable offence is involved (i.e., those offences of a more serious nature), TTC Special Constables must take instruction and direction from Police. If the alleged offence is not a dual procedure or indictable offence, the TTC Special Constables shall proceed to conduct the investigation. The Agreement further provides that the Police have primary responsibility for responding to and investigating serious occurrences on the transit system (e.g., violence involving weapons, violent incidents where injury has occurred or is likely to occur), while TTC Special Constables may respond to minor physical assaults not involving weapons or verbal confrontations. Finally, the Agreement provides that, for a specified list of offences that includes robbery, weapons, drugs, explosives and sexual offences, amongst others, the Police must be called and may investigate. The Police need not be called, however, where the alleged offence involves theft under $5000.

The Agreement provides that the TTC Special Constables shall be trained by the TTC in accordance with training standards prescribed by the Board for members.
of the Police, as modified for the TTC Special Constables considering their powers, duties and responsibilities.

Other factors which I find relevant include the following: TTC Special Constables may have access to confidential police information, such as CPIC and criminal record information; TTC Special Constables, although prohibited from carrying weapons and carrying out vehicle pursuits, may carry “pepper spray;” TTC Special Constables may make arrests and must transfer persons detained in custody to police; every arrest and investigation of a criminal offence conducted by a TTC Special Constable must be reported to the police.

Finally, the TTC must establish a complaints investigation procedure regarding the conduct of TTC Constables that corresponds to that of the Police, and must provide the Board with the results of all complaints investigations, as well as any information concerning misconduct or alleged misconduct. The Board may, if provided with a finding of misconduct or information regarding misconduct, suspend or terminate the appointment of a TTC Special Constable.

Considering the foregoing, and in particular the authority under section 53 of the Police Services Act and the powers, jurisdiction and procedures set out in the Agreement between the TTC and the Board, I am satisfied that the TTC Special Constables engage in “policing” and thus meet the definition of “law enforcement” under the Act. Although in certain contexts, the status and authority of the TTC Special Constables may be construed as subordinate to that of the Police, I nevertheless find that their activities are sufficiently similar to the Police such that they come within the meaning of “policing” under the “law enforcement” definition.

Finally, I am satisfied that when the video surveillance system is accessed on an incident driven basis to pursue an investigation by the TTC Special Constables it is “used for the purposes of law enforcement” and the underlying collection is therefore in compliance with the law enforcement condition of section 28(2).

Section 28(2) – Conclusion

I note that a given collection of personal information is permissible under the Act where it may be justified under at least one of the section 28(2) conditions. Based on the foregoing, I am satisfied that the collection of personal information through the video surveillance system is permitted under two of the section 28(2) conditions. The general collection is satisfied by the necessity condition, as well as the law enforcement condition with respect to the activities of the TTC Special Constables.

Having reached the conclusion that the collection of personal information through the use of video surveillance is permissible under section 28(2) of the Act, it is incumbent upon the TTC to govern its video surveillance system in a manner that places a high regard on the privacy of its passengers. While TTC passengers may
accept a certain degree of surveillance, they should not expect that their images or personal information will be improperly recorded or misused for purposes that are secondary to the purposes of safety and security. Therefore, for the remainder of this Report, I will focus on the governance aspects relating to the TTC’s use of video surveillance cameras.

**Conclusion:** The collection of personal information by the TTC’s video surveillance cameras is in compliance with section 28(2) of the Act.

**Issue C:** Is the Notice of Collection provided to passengers in accordance with section 29(2) of the Act.

Section 29(2) of the Act states:

If personal information is collected on behalf of an institution, the head shall inform the individual to whom the information relates of,

(a) the legal authority for the collection;

(b) the principal purpose or purposes for which the personal information is intended to be used; and

(c) the title, business address and business telephone number of an officer or employee of the institution who can answer the individual’s questions about the collection.

This section requires that institutions collecting personal information provide individuals with the Notice of Collection that is prescribed in section 29(2) of the Act. In the case of video surveillance programs, the Guidelines elaborate on the statutory requirement to provide a Notice of Collection and state:

The public should be notified, using clearly written signs, prominently displayed at the perimeter of the video surveillance areas, of video surveillance equipment locations, so the public has reasonable and adequate warning that surveillance is, or may be in operation before entering any area under video surveillance. Signs at the perimeter of the surveillance areas should identify someone who can answer questions about the video surveillance system, and can include an address, telephone number, or website for contact purposes.43

The Guidelines further state that while signs should contain the basic information relaying that individuals are under surveillance, the remainder of the notice requirement may be satisfied by having the entire notice appear in other media, such as in pamphlets and other printed materials.

With respect to the TTC’s video surveillance program, the TTC’s Policy contains the requirement that, “The TTC shall post signs, visible to members of the public, at all entrances and/or prominently displayed on the perimeter of the location being video recorded.” The Policy further states that the notice provided on the signs must contain the full notice requirement as set out in section 29(2) of the Act.

An appendix to the TTC’s Policy contains an illustration of the signs, which include a picture of a camera and the following text:

This area is being Video Recorded for Security Purposes.

The personal information collected by the use of video equipment at this location is collected under the authority of the City of Toronto Act, 2006 and the Occupiers’ Liability Act.

Any questions about this collection can be directed to the Coordinator, Freedom of Information/Records Management, at [phone number and contact information].

With respect to surface vehicles, the TTC has stated that a Notice of Collection decal containing the above wording has been posted on all vehicles in which cameras have been installed. With respect to the subway system, the TTC has acknowledged that signage containing the above wording has not yet been installed, but that plans are underway to install a total of 761 signs throughout the 69 stations. The TTC plans to install the signs as the use of video surveillance cameras expands.

I am satisfied that the Notice of Collection, as drafted, meets the requirements set out in section 29(2) of the Act and the Guidelines. I am also satisfied that the TTC’s plans with respect to the number and placement of signs are appropriate. However, it is imperative that the TTC ensure that signs are installed prior to the video surveillance cameras being activated at a particular site, and I will recommend that my office be advised of such developments.

**Conclusion:** The Notice of Collection provided to TTC passengers is in compliance with section 29(2) of the Act.

**Issue D: Is the disclosure of personal information to the Toronto Police Service in accordance with section 32 of the Act?**

The TTC has acknowledged that recorded video surveillance images collected from both surface vehicles and the subway system are disclosed to the Toronto Police Service (the Police) in response to requests for information about incidents involving criminal investigations. In addition, the TTC has stated that, in the future, the Police will have the ability to remotely access video surveillance images obtained from some of the cameras in the subway system, in accordance with the
MOU to be signed. The TTC provided a copy of the draft MOU to my office and indicated that the MOU would be signed once it is passed by the Toronto Police Services Board. This remote access by the Police also constitutes a disclosure of personal information on the part of the TTC, under the Act.

The rules relating to the disclosure of personal information are set out in section 32 of the Act, which states, in part:

An institution shall not disclose personal information in its custody or under its control except,

(a) in accordance with Part I;

(b) if the person to whom the information relates has identified that information in particular and consented to its disclosure;

(c) for the purpose for which it was obtained or compiled or for a consistent purpose;

(g) if disclosure is to an institution or a law enforcement agency in Canada to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result;

Section 32 establishes a basic prohibition on the disclosure of personal information, but states that there are certain circumstances under which the disclosure of personal information is permissible. In order for a given disclosure of personal information to be allowed under the Act, the institution in question must demonstrate that the disclosure in question is in accordance with at least one of the statutory exceptions set out in section 32. The TTC has cited various section 32 provisions to support its position that the disclosure to the Police is permissible.

In this case, there are generally two different types of disclosures of personal information taking place. The first is the physical disclosure of personal information to the Police (or another law enforcement agency) in response to an incident which may lead to criminal charges. The second type of disclosure is that which results from the direct remote access to video surveillance images of the TTC subway system by the Police.

With respect to the first type of disclosure, the physical disclosure of recorded video surveillance images to law enforcement officials in response to a specific incident, I note that these images may be taken from cameras located in both the subway system and on surface vehicles (including streetcars, once installed).
Privacy by Design

The TTC’s Policy describes the manner in which recorded images collected from the video surveillance cameras in both surface vehicles and the subway system are provided to law enforcement officials, in response to a specific incident:

If access to a video recording record is required for the purpose of a law enforcement investigation, the requesting Officer (or in emergency situations, the Operator that authorized the release) must complete the TTC’s Law Enforcement Officer Request Form ... and forward this form to the [Designated Departmental Management Staff] or designate [who] will provide the recording for the specified date and time of the incident as requested by the Law Enforcement Officer.

In my view, this type of disclosure of personal information, in response to a specific incident, where the requesting officer completes the prescribed form indicating a specific date, time and location of the incident being investigated, would constitute a “disclosure to an institution or a law enforcement agency in Canada to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result,” within the meaning of section 32(g) of the Act. Accordingly, I am satisfied that such disclosures are permissible under the Act.

The second type of disclosure (based on direct remote access to video surveillance images by the Police) is the subject of an MOU that has been drafted, but yet to be signed between the Toronto Police Services Board and the TTC. The draft MOU specifies that remote access to the video surveillance images shall only be permitted for law enforcement or public safety purposes and that no other uses are permitted without the express written consent of the TTC. The TTC stated that the remote access would take place from a computer, located within Police headquarters, connected to the TTC’s subway system through a fibre-optic cable. Access to the video surveillance images will be incident driven, requiring a case file number. Access will also be restricted to only eight designated individuals, within the Video Services Unit.

The initial draft of the MOU provided to my office indicated that the Police would have remote access to both live and recorded video surveillance images. My office was concerned that access to the live video surveillance feed by the Police could lead to potentially invasive activities and improper surveillance. During the course of the investigation, the TTC revised the draft MOU to restrict the Police’s remote access to recorded images only. Since the recorded images are only retained for a short period of time, I have less concern with this type of disclosure to the Police.
However, to ensure that each disclosure of personal information to the Police is for legitimate law enforcement and public safety purposes, all disclosures of personal information must be subject to stringent accountability and oversight. Accordingly, I recommend that prior to providing the Police with direct remote access to the recorded video surveillance images, the TTC should amend the draft MOU to require that the logs of disclosures to the Police be subjected to regular audits, conducted on behalf of the TTC. The TTC should provide my office with a copy of the revised draft MOU prior to signing.

**Conclusion:** The disclosure of personal information to the Toronto Police Services is in compliance with section 32 of the *Act*.

**Issue E: Does the TTC have adequate security measures in place to safeguard the personal information collected?**

Regulation 823, made pursuant to the *Act*, addresses the general security requirements for records in the custody of an institution. Section 3 of Regulation 823 states:

1. Every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected.

2. Every head shall ensure that only those individuals who need a record for the performance of their duties shall have access to it.

3. Every head shall ensure that reasonable measures to protect the records in his or her institution from inadvertent destruction or damage are defined, documented and put in place, taking into account the nature of the records to be protected.

The *Guidelines* elaborate on the security responsibilities of institutions operating video surveillance systems and state, in part:

- All tapes or other storage devices that are not in use should be stored securely in a locked receptacle located in a controlled-access area. Each storage device that has been used should be dated and labelled with a unique, sequential number or other verifiable symbol.

- Access to the storage devices should only be made by authorized personnel. Logs should be kept of all instances of access to, and use of, recorded material, to enable a proper audit trail. Electronic logs should be kept where records are maintained electronically.44

44 See *Guidelines*, page 8.
Under the section dealing with an institution’s video surveillance policy, the Guidelines state:

Employees should be subject to discipline if they breach the policy or the provisions of the Acts or other relevant statutes. Where a service provider fails to comply with the policy or the provisions of the Act, it would be considered a breach of contract leading to penalties up to, and including, contract termination.

Employees of institutions and employees of service providers should sign written agreements regarding their duties under the policy and the Acts, including an undertaking of confidentiality.45

Privacy International stated that there has been “insufficient consideration regarding access powers” on the part of the TTC. My office understood this comment to mean that Privacy International is of the view that, in implementing its video surveillance cameras, the TTC did not incorporate sufficient controls over who would have access to the live and recorded video surveillance images. With due respect, I disagree with this assertion. In materials provided to my office, the TTC described the security measures put in place to prevent unauthorized access to the images obtained through the video surveillance system.

With respect to the cameras located in TTC surface vehicles, the TTC noted that the hard drives containing the recorded video images are only accessible through the use of a password, which is only available to a limited number of TTC supervisors. The operators of TTC vehicles do not have any access to the recorded video images. The TTC stated:

In order to access, view and/or record extracted data a separate computer is required and can only be performed by authorized TTC personnel. To remove a recorder from a vehicle requires a special tool key, which is not available to operators. ... In addition, if a camera is moved, altered or in any way tampered with, the recorder creates an internal log indicating the occurrence and the time.

The TTC also provided a copy of a document entitled, Interim TTC Protocol for Surface Vehicle Safety Camera System, which documents the manner in which access may be granted to the recorded images collected by cameras located in surface vehicles in response to specific investigations.

The TTC has similar measures in place relating to the cameras located on the subway system. The TTC provided my office with a copy of written procedures describing the TTC’s internal process for requesting images recorded at a given site

45 See Guidelines, page 5.
within the subway system. These procedures describe the way in which recorded images may be used internally, the staff designations who may have access to them, and the manner in which access may be provided. The TTC also noted that all designated staff permitted access to recorded images must receive training on privacy and security:

All TTC personnel that access recorded video images are required to log all activities relating to such access, including the time and purpose. A log book is maintained within each station … [E]ach recorder also creates its own internal log every time the recorder is accessed or an image is accessed.

Further, the TTC has stated:

Cameras located within a specific subway station simultaneously transfer images to a recorder located within a secure room and area of the subway station. All recorders are in a locked cabinet, in a restricted access room.

In my view, the security measures in place, based on the information contained in the TTC’s Policy, the written procedures, as well as other information provided, are comprehensive. However, I note that the TTC’s Policy does not contain the requirement, as set out in our Guidelines, that all employees dealing with the video surveillance system must sign written agreements regarding their duties under the Policy and the Acts, including an undertaking of confidentiality. Accordingly, the TTC should amend the Policy to incorporate such wording to fully satisfy its responsibilities relating to security of recorded information under Regulation 823 and the Guidelines.

**Conclusion:** The TTC has adequate security measures in place to safeguard the personal information collected. However, the TTC should amend its Policy to require that all employees dealing with the video surveillance system sign a written agreement regarding their duties, including an undertaking of confidentiality.

**Issue F: Does the TTC have proper destruction processes in place for recorded information that is no longer in use?**

As discussed above, Regulation 823 requires that institutions have proper security safeguards in place to protect records from unauthorized access. The principle that unauthorized access should be prevented applies to all aspects of a record’s life cycle, up to, and including, its destruction.

The Guidelines address the destruction of records that have been created through the use of video surveillance in the past and state:
Old storage devices must be securely destroyed in such a way that the personal information cannot be reconstructed or retrieved. Destruction methods could include overwriting electronic records, shredding, burning or magnetically erasing the personal information.\footnote{See \textit{Guidelines}, page 9.}

In sum, the \textit{Guidelines} recommend the secure destruction of all recorded video images.

With respect to the images collected from surface vehicles, the TTC stated that the system is designed to automatically overwrite every 15 hours. Since actual recording only takes place when the vehicle is in operation, the images will be deleted and overwritten with new images at least every 24 hours.

The TTC’s Policy addresses the secure destruction of video records, and states:

> The TTC will take all reasonable efforts to ensure the security of records in its control/custody and ensure their safe and secure disposal. Old storage devices must be disposed of in accordance with an applicable technology asset disposal process ensuring personal information is erased prior to disposal, and cannot be retrieved or reconstructed. Disposal methods may include shredding, burning, or erasing depending on the type of storage device.

In addition to the general destruction requirements expressed in the Policy, the TTC has also provided specific information on the secure destruction of recorded images. With respect to images taken from recorders located on surface vehicles, the TTC stated:

> If a request for images is received, the images are downloaded from the digital video recorder to an investigation station (laptop computer). If the images are to be retained, the images are burned from a laptop computer to a DVD. All laptop computers which contain appropriate software to download video recorded information from vehicles are equipped with a file shredding application which shreds each downloaded file upon being activated by the authorized TTC supervisor.

With respect to the images recorded from the subway system, the TTC stated that images are retained in a controlled-access area of any given subway station. Images are retained for a maximum retention period of seven days, and then overwritten.

In light of the information provided by the TTC, I am satisfied that the destruction methods for images retained from video surveillance cameras are appropriate and in compliance with the requirements under our \textit{Guidelines}. I am also satisfied that
these destruction methods constitute “reasonable measures” to protect the security of recorded images under section 3 of Regulation 823.

**Conclusion:** The TTC has proper destruction processes in place for recorded information that is no longer in use.

**Issue G: Does the TTC have proper retention periods in place for personal information that is collected?**

Section 5 of Regulation 823 establishes a minimum retention period for personal information that has been collected by an institution, and states:

> Personal information that has been used by an institution shall be retained by the institution for the shorter of one year after use or the period set out in a by-law or resolution made by the institution or made by another institution affecting the institution, unless the individual to whom the information relates consents to its earlier disposal.

This provision establishes a minimum one-year retention period for personal information that has been “used.” The purpose of this provision is to require that institutions maintain records containing personal information for at least one year in order to facilitate a right of access by individuals to their own personal information.

I note that the one-year retention requirements for records that have been used are not currently expressed in the Policy or in materials provided to my office. Accordingly, I will be recommending that the TTC incorporate the appropriate retention periods into the Policy before it is finalized.

The Guidelines elaborate on the retention requirement in the Regulation and recommend a retention period for video surveillance images that have been collected but have not been used, and state:

- The organization should develop written policies on the use and retention of recorded information that:
  
  - Set out the retention period for information that has not been viewed for law enforcement or public safety purposes. Recorded information that has not been used in this fashion should be routinely erased according to a standard schedule (normally between 48 and 72 hours).
  
  - Establish a separate retention period when recorded information has been viewed for law enforcement or public safety purposes.47
  
47 See Guidelines, page 8.
In the Policy, the TTC has not finalized the retention period for recorded images collected from video surveillance cameras. However, in materials provided to my office, and addressed above, the TTC has stated that images recorded from surface vehicles would be overwritten after 15 hours if the image had not been used as part of an investigation. For the subway system, images will be overwritten after a period of seven days, if not used.

The TTC has provided my office with Transport Canada’s *Closed Circuit Television Reference Manual for Security Applications*, which recommends retention periods of between seven and 30 days for images recorded from video surveillance cameras. My office’s *Guidelines* recommend a shorter retention period of 72 hours. Video surveillance cameras operated by the Police in the entertainment district of downtown Toronto currently operate successfully with a maximum retention period of 72 hours and have operated on this basis for several years. In my view, 72 hours provides a sufficient window of time for the TTC and the Police to determine if an incident has occurred and if video surveillance footage may be relevant to its investigation. Therefore, I see no reason to extend the retention period beyond the recommended 72 hours.

**Conclusion:** The TTC should amend its retention periods for video surveillance images that have not been used from the current maximum of seven days to a maximum of 72 hours.

**Issue H: Has the TTC undertaken all appropriate steps prior to implementing video surveillance?**

With respect to Privacy International’s assertion that the “scheme is being deployed without consideration of privacy and associated protocols,” I note that the TTC’s draft Policy has actually been modelled on the recommended provisions outlined in my office’s *Guidelines for the Use of Video Surveillance Cameras in Public Places*, which are intended to provide direction on the deployment of video surveillance in a privacy-protective manner. The TTC has been careful to ensure that the key privacy provisions of the *Guidelines* have been incorporated into their draft Policy.

Our *Guidelines* provide recommendations regarding the steps that institutions should take prior to engaging in video surveillance.

The *Guidelines* state, in part:

- An assessment of privacy implications should be conducted on the effects that the proposed video surveillance system may have on personal privacy, and the ways in which any adverse effects can be mitigated by examining the collection, use, disclosure and retention of personal information.
Consultations should be conducted with relevant stakeholders as to the necessity of the proposed video surveillance program and its acceptability to the public. Extensive public consultation should take place.48

As discussed above, the TTC has engaged in public consultation on certain elements of its video surveillance system. For instance, the TTC has sought the public’s opinion on the design of new streetcars, and invited the public to provide comment on mock-ups of the new subway cars. In both cases, the presence of video surveillance cameras was considered to be positive by those involved in the consultation process.

With respect to the requirement that the TTC conduct a formal assessment into privacy impacts, the TTC noted that, as an Appendix, the Policy contains a Surveillance Video Security Threat Assessment. The TTC noted that a formal threat assessment will be completed prior to the finalization of its Policy, which is planned for early 2008.

The IPC Guidelines recommend “extensive” public consultation to ensure that stakeholders are educated and informed of the video surveillance system and given an opportunity to provide feedback. While the TTC has undertaken some consultations, these consultations were not specific to the TTC’s overall video surveillance program. I am not convinced that these consultations fulfill the requirements of our Guidelines and have concluded that the steps taken prior to the implementation of video surveillance by the TTC, specifically with respect to extensive public consultation, are not sufficient.

As the TTC continues to expand its video surveillance program, I recommend that more public consultations take place, possibly in the form of town hall meetings, to broadly educate the public and publicize the expansion of the video surveillance system in Toronto’s public transit system. In addition to conducting public consultations, I recommend that the TTC inform the public of its video surveillance program by publishing general information on its website and in printed materials, as appropriate.

Conclusion: As the TTC expands the use of video surveillance cameras in the public transit system, it must take additional steps to inform the public, by publishing general information on its website and by holding more extensive consultations, possibly in the form of town hall meetings.

Issue I: Is the TTC’s video surveillance system subject to regular audits?

In the context of video surveillance, an audit should be viewed as a thorough examination of an institution’s policies, practices and procedures, as well as a test of internal compliance with the obligations set out under these documents. The audit requirement is expressed in our Guidelines as follows:

Organizations should ensure that the use and security of video surveillance equipment is subject to regular audits. The audit should also address the organization’s compliance with the operational policies and procedures. An external body may be retained in order to perform the audit. Any deficiencies or concerns identified by the audit must be addressed immediately.

Employees and service providers should be aware that their activities are subject to audit and that they may be called upon to justify their surveillance interest in any given individual.49

The general utility of organizational privacy audits has been recognized by the Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certified Public Accountants (AICPA), who have jointly published their Generally Accepted Privacy Principles (GAPP) – A Global Privacy Framework (the GAPP Privacy Framework).50 The GAPP Privacy Framework was developed to assist organizations in identifying and managing privacy risks and serves as an excellent basis for conducting independent audits.

The TTC has developed comprehensive policies and procedures that seek to minimize improper access and intrusions into the privacy of individuals. The systems described above, which contemplate defined staff privileges and a paper trail of access documented through logs, are also intended to prevent potential abuses of their surveillance system.

Notwithstanding these protections, the size and complexity of the TTC as an organization, as well as the extent of surveillance due to the number of cameras in operation, gives rise to the potential for abuse. Accordingly, regular system-wide audits (at least on an annual basis) will help to ensure that the system is operating properly with respect to privacy and will help to reduce the risk of a privacy breach.

In the materials provided to the IPC, the TTC made reference to plans for conducting annual audits of their surveillance system. In the Policy, under the section “Roles and Responsibilities,” the General Secretary of the TTC is listed as being responsible for ensuring Policy compliance and for coordinating annual audits of the TTC’s video surveillance system.

The TTC’s Policy provides no further elaboration of these audits. There is no separate heading for audits in the Policy nor is there any reference to the requirement that audits be conducted on an annual basis.

Accordingly, I am recommending that the TTC amend its Policy in order to make the audit requirement more explicit. I am also recommending that the TTC provide

49 See Guidelines, page 10.
50 The GAPP Framework is available from the CICA’s website: http://www.cica.ca/index.cfm/ci_id/36529/la_id/1
a copy of its first annual audit to the IPC’s Policy Department for review. Review by my office will help to ensure that the audit is methodologically sound and comprehensive in its scope. In addition, the initial audit should be performed by an independent third party using the GAPP Privacy Framework and should also assess the TTC’s compliance with the recommendations made in this Report. This will allow my office to follow up on any shortcomings identified through the audit.

**Conclusion:** The TTC must ensure that its video surveillance program is subjected to an effective and thorough audit conducted by an independent third party, using the GAPP Privacy Framework.

**Summary of Conclusions**

In summary, I have made the following conclusions in this investigation:

A The information collected by the TTC’s video surveillance cameras qualifies as “personal information” as defined under section 2(1) of the Act.

B The collection of personal information by the TTC’s video surveillance cameras is in compliance with section 28(2) of the Act.

C The Notice of Collection is provided to TTC passengers in compliance with section 29(2) of the Act.

D The disclosure of personal information to the Toronto Police Services is in compliance with section 32 of the Act.

E The TTC has adequate security measures in place to safeguard the personal information collected. However, the TTC should amend its Policy to require that all employees dealing with the video surveillance system sign a written agreement regarding their duties, including an undertaking of confidentiality.

F The TTC has proper destruction processes in place for recorded information that is no longer in use.

G The TTC should amend its retention periods for video surveillance images that have not been used from the current maximum of seven days to a maximum of 72 hours.

H As the TTC expands its use of video surveillance cameras in the public transit system, it must take additional steps to inform the public, by publishing general information on its website and by holding more extensive consultations, possibly in the form of town hall meetings.

I The TTC must ensure that its video surveillance program is subjected to an effective and thorough audit conducted by an independent third party, using the GAPP Privacy Framework.
Re commendations

In light of the conclusions contained in this Report, I recommend that the TTC take the following steps to enhance the protection of personal information collected through its video surveillance system. Specifically, I make the following recommendations:

1. That, prior to providing the Police with direct remote access to the video surveillance images, the TTC should amend the draft MOU to require that the logs of disclosures be subjected to regular audits, conducted on behalf of the TTC. A copy of the revised draft MOU should be provided to my office prior to signing.

2. That the TTC amend its Policy to reflect the conditions set out in the revised MOU.

3. That the TTC amend its Policy to require that all employees dealing with the video surveillance system sign a written agreement regarding their duties, including an undertaking of confidentiality.

4. That the TTC advise my office of its progress in installing the signs providing Notice of Collection to passengers.

5. That the TTC amend its retention periods for video surveillance images from a maximum of seven days to a maximum of 72 hours.

6. That the TTC amend its Policy to include applicable retention periods, both for when images are used (minimum of one year) and when the images are not used (either 15 hours or 72 hours, depending on where the camera is situated).

7. As the TTC expands its use of video surveillance cameras in the public transit system, it must take additional steps to inform the public, by publishing general information on its website and by holding more extensive consultations, possibly in the form of town hall meetings.

8. That the TTC include an additional heading in its Policy specifically addressing the annual audit requirement. The Policy should state that the annual audit must be thorough, comprehensive, and must test all program areas of the TTC employing video surveillance to ensure compliance with the Policy and the written procedures. The initial audit should be conducted by an independent third party, using the GAPP Privacy Framework, and should include an assessment of the extent to which the TTC has complied with the recommendations made in this Report.
9 That the TTC provide my office with a copy its first annual audit for review, and comment on the details and methodology of the audit.

10 That the TTC provide my office with a copy of its revised Policy no later than one month after the date of this Report.

11 That the TTC should keep abreast of research on emerging privacy-enhancing technologies and adopt these technologies, whenever possible.

12 That the TTC should select a location to evaluate the privacy-enhancing video surveillance technology developed by the University of Toronto researchers K. Martin and K. Plataniotis.

13 Within three months of the date of this Report, the TTC should provide my office with proof of compliance or an update on the status of its compliance with each of these recommendations.

Commissioner’s Message

The area of video surveillance presents a difficult subject matter for privacy officials to grapple with impartially because, on its face, it is inherently privacy-invasive, due to the potential for data capture. Despite that fact, there are legitimate uses for video surveillance, as outlined in this Report, that render it in compliance with our privacy laws. The challenge we thus face is to rein in, as tightly as possible, any potential for the unauthorized deployment of the system. We have attempted to do this by ensuring that strong controls are in place with respect to its governance (policy/procedures), oversight (independent audit, reportable to my office) and, the most promising long-term measure, the introduction of innovative privacy-enhancing technologies to effectively eliminate unauthorized access or use of any personal information obtained.

In light of the growth of surveillance technologies, not to mention the proliferation of biometrics and sensoring devices, the future of privacy may well lie in ensuring that the necessary protections are built right into their design. “Privacy by design” may be our ultimate protection in the future, promising a positive-sum paradigm instead of the unlikely obliteration of a given technology. My goal is to have privacy embedded into the architecture of all future technologies, thereby preserving it well into the future.

Ann Cavoukian, Ph.D.
Commissioner
Biometric Encryption:
A Positive-Sum Technology That Achieves
Strong Authentication, Security, and Privacy

March 2007
Abstract

This paper discusses privacy-enhanced uses of biometrics, with a particular focus on the privacy and security advantages of Biometric Encryption (BE) over other uses of biometrics. The paper is intended to engage a broad audience to consider the merits of the Biometric Encryption approach to verifying identity, protecting privacy, and ensuring security. Our central message is that BE technology can help to overcome the prevailing “zero-sum” mentality, namely, that adding privacy to identification and information systems will necessarily weaken security and functionality. This paper explains how and why BE technology promises a “positive-sum,” win-win scenario for all stakeholders involved.

Background/Context

Identification and authentication requirements are steadily increasing in both the online and off-line worlds. There is a great need on the part of both public and private sector entities to “know” who they are dealing with. The current security model for the verification of identity, protection of information, and authorization to access premises or services is based on using a token, tied to and thereby representing an individual, to either authenticate identity or allow access to information, premises or services. This token may be a password or shared secret (something you know), an identity card (something you have), or a biometric (something you are). In all of these cases, the details of the token are held by a third party whose function is to authorize and, at times, allow the transaction to proceed if the details of an individual’s token match those stored in a database. The biometric is increasingly viewed as the ultimate form of authentication or identification, supplying the third and final element of proof of identity. Accordingly, it is being rolled out in many security applications.

Privacy-related areas involving the protection of personal information, however, are not as strong – biometrics have not yet been able to fill this need. When an individual provides his or her personal information (financial or medical) to a second party, this party often stipulates that it will only use the personal information for the agreed-upon function, and will thereafter protect the information from access by unauthorized parties. The relationship between the individual who provides the information and the second party is largely based on a model of trust.
The trust model is becoming far less effective as current technological and geopolitical situations evolve. The selling or sharing of personal information is now a lucrative business model practised by many companies. Similarly, with increased threats of terrorism, governments and law enforcement agencies can now demand access to more and more personal information. With the growing powers of the Internet, extensive electronic dossiers may now be developed about an individual, without his or her knowledge or consent. Of even greater concern, perhaps, are the errors that can easily arise, which may then adversely affect that individual’s life.

These dossiers may also include the details of token-based transactions such as biometrics, resulting in surprisingly complete dossiers about individuals and their transactional histories, again without their knowledge or consent. In turn, this precludes one’s ability to ever correct any errors which may be contained in such databases, presenting an ever-growing problem. In short, unauthorized access to one’s personal information can result in a host of negative consequences, ranging from identity theft and harassment to the perpetuation of mistakenly used personal information.

We acknowledge that government and law enforcement agencies require personal information to protect public safety and national security, while businesses require personal information to improve business practices and customer service. However, within these scenarios, the existing model of protecting privacy and safeguarding information invariably leads to a zero-sum game – protecting privacy often leads to less security and more costly business practices. This need not be the case.

Protecting public safety and a nation’s security is a necessary and important function of a civilized society; developing more efficient business practices that are more cost effective and lead to better customer service are also highly desirable. Social and economic well-being are served by both of these functions.

However, liberty and freedom of choice are also essential to the functioning of prosperous and free societies. Technological advances in the collection and processing of information over the last few decades have positioned this resource as vital to the health, well-being and freedom of individuals. More specifically, abuses of personal information can cause untold harm, wasted resources, and generally lead to the detriment of society. For example, a society of individuals perpetually anxious about identity theft, misuses of their information, or unwarranted search and seizures cannot function at optimum levels.

It is our belief that the security model in current use must change from a zero-sum to a positive-sum paradigm, where both the need for privacy/protection of personal information and the need for security can be satisfied. Accordingly, in this paper, we present what we believe to be the first step in the achievement of that goal through a new positive-sum model for both protecting information and providing security, based on “Biometric Encryption.”
Biometric Encryption: A Positive-Sum Technology That Achieves Strong Authentication, Security, and Privacy

Growing Public Awareness and Interest
Biometrics are expected to add a new level of security to applications, as a person attempting access must prove who he or she really is by presenting a biometric to the system. Such systems may also have the convenience, from the user’s perspective, of not requiring the user to remember a password.

There is evidence of growing public awareness and interest in the use of biometrics.

Border Security Control: Perhaps the most visible (and controversial) use of biometrics is taking place in the transportation sector. Identification requirements at airports and border crossings may now involve the collection and processing of travellers’ fingerprints, facial images, and iris patterns. Increasingly, machine-readable travel documents such as passports, driver’s licences, and other identity or travel cards may also contain biometric data or images. Frequent travellers who apply for and pass extensive background checks may use their biometrics for speedy passage through customs and immigration.

Crime and Fraud Prevention, Detection, and Forensics: The use of fingerprints by law enforcement has taken place for many years, but now that fingerprints can be digitized, stored, retrieved, and matched instantaneously, many new uses have emerged, such as for populating watch lists and carrying out private sector background checks. In some parts of the United States, cashing a cheque can require a biometric imprint to be placed on the obverse side. Not a day goes by where the public is not apprised of some new “revolutionary” biometric technology that promises to solve crimes, catch villains, and generally make the world a better place to live.

Attendance Recording: Employees and students are being required, in growing numbers, to present a biometric (such as a finger or hand) in order to “check in” to premises, much like a punchclock, or to claim some entitlement such as a luncheon meal or to check out a library book.

Payment Systems: We are seeing increasing uses of biometrics by the private sector for enhanced convenience services, such as “pay ’n’ go” systems that allow enrolled customers to pay for groceries or gasoline using only their finger – at times, an enormous convenience.

Access Control: One of the most widespread uses of biometrics has been for physical and logical access to secure areas or resources (e.g., to a database of medical records, or accessing a laptop). In such circumstances, biometrics can enhance security by helping to ensure that access to sensitive resources is strictly restricted to authorized individuals.
A Biometrics Primer

“Biometrics” refers to automatic systems that use measurable, physical or physiological characteristics or behavioural traits to recognize the identity, or verify/authenticate the claimed identity of an individual. The examples of biometric characteristics that have been used for automated recognition include fingerprints, iris, face, hand or finger geometry, retina, voice, signature, and keystroke dynamics.

These systems are based on the following steps: a biometric sample is taken from an individual, for instance a fingerprint or iris scan. This physical characteristic may be presented by an image. Often data are extracted from that sample. These extracted data constitute a biometric template. The biometric data, either the image or the template or both, are then stored on a storage medium. The medium could be a database or a distributed environment, such as smart cards. These preparatory phases together constitute the process of enrolment. The person whose data are thus stored is called the enrollee.

The actual purpose of the biometric system is only achieved at a later stage. If a person presents herself to the system, the system will ask her to submit her biometric characteristic(s). The system will then compare the image of the submitted sample (or the template extracted from it) with the biometric data of the enrollee. If the match succeeds, the person is then recognized and the system will “accept” her. If the match does not succeed, she is not recognized and she will be “rejected.”

Traditional Biometrics: Privacy vs. Security – A Zero-Sum Game

We thought it might be useful to begin with a table (see next page) that summarizes the essential differences between the traditional zero-sum approach to biometrics vs. the positive-sum, Biometric Encryption approach. Such a comparison facilitates ease of reference and differentiates one from the other; this is also followed by the page number where a full discussion of the issue takes place.

Applicable law and regulation will vary, but biometric data, being derived from human bodies (and especially when used to identify or verify those bodies) is considered personally identifiable information (PII). The collection, use, and disclosure of biometric data – image or template – invokes rights on the part of an individual and obligations on the part of an organization.

Difficult ethical and operational questions surround the collection and use of video images used for facial recognition (which may be collected without the knowledge or consent of the individual), and of fingerprints and DNA samples, which may also reveal far more than identity.

As biometric uses and databases grow, so do concerns that the personal data collected will not be used in reasonable and accountable ways. Privacy concerns arise when biometric data are used for secondary purposes, invoking “function
<table>
<thead>
<tr>
<th>Traditional Biometrics: Privacy or Security – A Zero-Sum Game</th>
<th>Biometric Encryption: Privacy and Security – A Positive-Sum Game</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  The biometric template stored is an identifier unique to the individual.</td>
<td>There is no conventional biometric template; therefore no unique biometric identifier may be tied to the individual. (pp. 127, 128)</td>
</tr>
<tr>
<td>2  Secondary uses of the template (unique identifier) can be used to log transactions if biometrics become widespread.</td>
<td>Without a unique identifier, transactions cannot be collected or tied to an individual. (pp. 128, 129, 138)</td>
</tr>
<tr>
<td>3  A compromised database of individual biometrics or their templates affects the privacy of all individuals.</td>
<td>No large databases of biometrics are created, only biometrically encrypted keys. Any compromise would have to take place one key at a time. (p. 135)</td>
</tr>
<tr>
<td>4  Privacy and security not possible.</td>
<td>Privacy and security easily achieved. (pp. 128-132, 139-142)</td>
</tr>
<tr>
<td>5  Biometric cannot achieve a high level of challenge-response security.</td>
<td>Challenge-response security is an easily available option. (pp. 139-141)</td>
</tr>
<tr>
<td>6  Biometrics can only indirectly protect privacy of personal information in large private or public databases.</td>
<td>BE can enable the creation of a private and highly secure anonymous database structure for personal information in large private or public databases. (pp. 130-131, 140-141)</td>
</tr>
<tr>
<td>7  1:many identification systems suffer from serious privacy concerns if the database is compromised.</td>
<td>1:many identification systems are both private and secure. (pp. 128, 131)</td>
</tr>
<tr>
<td>8  Users’ biometric images or templates cannot easily be replaced in the event of a breach, theft, or account compromise.</td>
<td>Biometrically encrypted account identifiers can be revoked and a new identifier generated in the event of breach or database compromise. (p. 129)</td>
</tr>
<tr>
<td>9  Biometric system is vulnerable to potential attacks.</td>
<td>BE is resilient to many known attacks. (p. 129)</td>
</tr>
<tr>
<td>10 Data aggregation.</td>
<td>Data minimization. (p. 128)</td>
</tr>
</tbody>
</table>
creep,” data matching, aggregation, surveillance and profiling. Biometric data transmitted across networks and stored in various databases by others can also be stolen, copied, or otherwise misused in ways that can materially affect the individual involved.

A broad discussion of the various privacy implications of biometrics is available on the website of the Information and Privacy Commissioner of Ontario, www.ipc.on.ca.

**Biometric Identification vs. Verification**

Regardless of specific uses and deployment scenarios, most biometric systems will serve one of two foundational purposes: **identification** or **verification/authentication**.

**Identification** refers to the ability of a computer system to uniquely distinguish an individual from a larger set of individual biometric records on file (using only the biometric data). So, theoretically, a national biometric identification system could allow a citizen to prove who he or she is without recourse to any document – assuming the citizen was already registered in the system. The presented biometric data would simply be compared with all other entries in the national database for a match, and upon a successful match the associated citizen's identity data would be released from the database. This is often referred to as a “one-to-many” match, and is used by police to identify criminals on watchlists, as well as by governments to identify qualified recipients for benefit-entitlement programs and registration systems such as voting, driver’s licence, and other applications. So, for example, the facial images supplied in support of passport or driver’s licence applications could be routinely compared against large databases to ensure that multiple documents had not been issued to the same applicant (i.e., fraud detection).

**Biometric verification** or authentication involves a “one-to-one” search whereby a live biometric sample presented by a person is compared with a stored sample (on a smart card or contained in a database) previously given by that individual, and the match confirmed. The eligibility of the person for the service or benefit has already been previously established. The matching of the live biometric to the sample is all that is necessary to authenticate the individual as an eligible user. There need not be any search or matching to a central database, although a central database can still be used, provided that some other identification data is used. For example, an identity card’s serial number could be used to “look up” an individual in a biometric database, and the live biometric sample could then be matched against the sample stored on record to verify the individual as the rightful bearer of the card. Even simpler, the person could just type in his username, so that his biometric template could be called up from the database for verification.

1 e.g., “Privacy and Biometrics,” “Biometrics and Policing: Comments from a Privacy Perspective,” and “Biometrics and Consumer Applications.” All documents are freely available at www.ipc.on.ca
Identification templates are always stored in a database that is controlled by a custodian. One-to-one templates can be stored either in a database or in a distributed medium carried by a user (e.g., a passport, a smart card, or token). In the latter case, the user retains control over his biometric template.

Some current deployments require both identification and verification. For example, if a person applies for a passport/ID card, his biometric samples enter a one-to-many search first. This is done to check his background, i.e., to make sure that the person has not been listed in a criminal/terrorist database before, usually under different identity. If the person is cleared, he is issued the passport/ID card to be used in a one-to-one system later on.

Somewhere between “one-to-many” identification and “one-to-one” authentication lies “one-to-few” biometric data uses, where “few” is of an order of 2–10,000. For example, a biometric lock may store the templates from all the members of a household or a firm. Some tokenless access control systems operate on this basis: the employee or user simply presents a biometric sample to the system, which then compares the sample against a small database of authorized users. If a match occurs, access is granted. The individual is both “identified” and “verified” as an authorized user – no other form of identification takes place.

Problems with Using Biometrics for Identification Purposes

In the futuristic film Minority Report, starring Tom Cruise, individuals are automatically and instantaneously identified via a millisecond remote scan of their irises. To escape detection, individuals must literally change their eyeballs. Thankfully, this scenario isn’t likely to happen for some time because, for various reasons, biometric technologies are not well suited for large-scale one-to-many real-time identification purposes.

It is important to bear in mind that the collection of biometric samples and their processing into biometric templates for matching is subject to great variability. Simply put, biometrics are “fuzzy” – no two samples will be perfectly identical. Facial recognition technologies, for example, are notoriously prone to variability due to different lighting conditions, angle, subject movement, and so forth. This is the reason, for example, that we are asked not to smile in our passport photos. Similarly, numerous factors affect the ability to obtain reliable and consistent fingerprint samples. Among the various biometric types, irises seem to be the most accurate and consistent.
Privacy by Design

As a consequence, live biometric samples can be at some variance with stored reference samples, making comparison, matching, and identification an inexact process. In other words, biometric systems do not have 100 per cent accuracy. When the biometric system cannot perform a proper match and (incorrectly) rejects a legitimate user, this is called a false reject, and the user must typically resubmit one or more biometric samples for further comparison by the system.

Biometric system designers can and do take measures to lower the false rejection rate (FRR) of their systems so this variability is smoothed out and the system can function properly. Apart from controlling the conditions under which fresh samples are taken, and improving the mathematical algorithms, one way to do this is to lower the threshold for matches to occur. However, the difficulty with this approach is that this often increases the false acceptance rate (FAR) of the system, that is, the system will incorrectly match a biometric to the wrong stored reference sample, resulting in misidentification. Usually there is a tradeoff between FRR and FAR, i.e., one error rate may only be reduced at the expense of the other (for example, some applications require lower FRR but can tolerate higher FAR, and vice versa).

The FRR/FAR numbers quoted by biometric vendors are often unreliable. The reader is advised to consult reputable independent sources of information, such as, for example, biometric competitions organized by the U.S. National Institute of Standard (NIST)\(^2\), or International Fingerprint Verification Competitions (FVC2000/2002/2004)\(^3\). For most biometric systems, FRR ranges from 0.1\% to 20\%, meaning that a legitimate user will be rejected from one out of 1,000 times to one out of five times on average. FAR ranges from one in 100 (low security applications) to one in 10,000,000 (very high security applications).

Other challenges for a biometric system are speed (the system must make an accurate decision in real time), and security (the system must be resilient against attacks).

So far, we have presented a straightforward technical discussion of the critical concepts of FAR and FRR. Now we will consider the operational consequences and impacts of these rates for one-to-many identification purposes.

Assume, for example, a biometric identification system with a 0.01\% FRR and 0.0001\% FAR (an unlikely high accuracy, we acknowledge). That is, the system is able to consistently match a genuine biometric sample 9,999 times out of 10,000 attempts on average. As remarkably efficient as this system sounds, a single biometric sample, when compared against a database of 1,000,000 samples, will generate on average one false accept in addition to one exact match (if the user was actually enrolled in the database).

\(^{3}\) http://bias.csr.unibo.it/fvc2004/
Now assume a database of 30,000,000 entries; each biometric sample would generate about 30 false accepts, each and every time! Clearly, this would be unacceptable for any real-time automatic identification system and would require significant human intervention in order to function.

Consequently, biometric system designers have resorted to other techniques to overcome the inherent technological problems of \textit{one-to-many} identification. One way to significantly improve accuracy is to collect and compare \textit{multiple} biometric samples. Multi-modal biometrics, for example, can involve collecting and using two (or more) fingerprints instead of one. If one fingerprint generates dozens or hundreds of false accepts, then the likelihood that two fingerprints will falsely match others in the database diminishes considerably. This is the primary reason behind emerging international requirements for including two separate biometrics (face and finger, for example), in machine-readable travel documents such as passports.

The privacy issue here, of course, involves the fact that more and more biometric samples of personal information need to be collected, transmitted, stored, and processed in order for the system to function properly. The FBI Integrated Automated Fingerprint Identification System (AFIS), containing hundreds of millions of records, for example, uses all 10 fingerprints for increased accuracy and speed. The US-VISIT program also plans to migrate from two fingerprints to 10 fingerprints and to develop the interoperability between US-VISIT and IAFIS.\footnote{http://www.gao.gov/new.items/d07278.pdf}

Significant privacy (and operational) concerns arise with unrestricted collection and use of more and more biometric data for identification purposes. To begin with, the creation of large centralized databases, accessible over networks in real time, presents significant operational and security concerns.

If networks fail or become unavailable, the entire identification system collapses. Recognizing this, system designers often build in high redundancy in parallel systems and mirrors (as well as failure and exception management processes) to ensure availability. However, this can have the effect of increasing the security risks and vulnerabilities of the biometric data.

Large centralized databases of biometric PII, hooked up to networks and made searchable in a distributed manner, represent significant targets for hackers and other malicious entities to exploit. It is also a regrettable reality that large centralized databases are also more prone to function creep (secondary uses) and insider abuse. There are also significant risks associated with transmitting biometric data over networks where they may be intercepted, copied, and actually tampered with, often without any detection.
Privacy by Design

Some large-scale biometric identification databases (such as the IAFIS, cited above) not only collect and file multiple biometric samples but, in an effort to preserve maximum compatibility with other fingerprint identification systems, store the full and complete images of the biometrics involved in addition to the templates! Proposed international standards for biometric-enabled machine-readable travel documents, for example, call for storage of the biometric images in the document rather than a structured reduction of the biometric into a unique template, in order to facilitate cross comparison and identification with other databases.

Storing, transmitting and using biometric images only exacerbates the privacy concerns with large-scale identification systems, since a very important privacy protection afforded by templates is removed, namely, the inability to exactly reconstruct the original biometric image from the template.

The image, conversely, can be converted into hundreds of templates for matching and identification (or other unknown or illegal) purposes, such as creating personal profiles and, let us not forget, committing identity theft. At this point, the privacy implications explode.

It should be evident that the loss or theft of one’s biometric image opens the door to massive identity theft if the thief can use the biometric for his or her own purposes. For example, the ability to create low-cost duplicate fake fingerprints from “gummy bears,” which are capable of fooling nine out of 10 biometric systems, has been well documented. Others have even documented how easy it is to fool a biometric system by presenting it with a photograph! Of course, the biometric industry has come up with countermeasures, such as “liveness detection” of a finger, or capturing 3D face images, but so will the attackers in this perpetual game. Moreover, in the digital realm, there may be no need to even present a “fake finger” if all that is required is the digital equivalent, which can be supplied to the network instead.

Even worse, in all of these identification scenarios, the biometric effectively serves as an index or key to the database involved, much like login usernames serve to identify registered users of a computer network.

But, because people usually only have two thumbs, two eyes, and one head, it is nearly impossible to change these if and when the related biometric data become compromised. In this sense biometrics operate like shared secrets or passwords – learn the secret and you’re in! But there are some very important differences between biometrics and passwords: you cannot change them and have no choice but

---

to keep them for life. Lose control of your lifetime password and you will have some explaining to do! This, regardless of the fact that security experts roundly condemn using unchangeable passwords as shared secrets (e.g., birthdates and SINs).

**Views of the Privacy Community**

The global privacy and data protection community have consistently argued *against* the use of biometrics for most one-to-many identification purposes, and *against* the creation of large, centralized or interoperable databases of biometric data:

- Resolution of International Data Protection Authorities;⁶
- Opinions of the European EDPS and Article 29 Working Party;⁷ and
- Publications and testimony of Ontario Information and Privacy Commissioner.

The global privacy community has insisted on building privacy-enhancing technologies (PETs) directly into biometrics systems wherever possible, to ensure that they reflect the requirements of Fair Information Principles and Practices and applicable privacy laws regarding the collection, use and disclosure of PII. Privacy, consumer, and civil rights advocates around the world have strongly favoured limiting the use of biometrics for verification/authentication purposes, especially in distributed environments (where the biometric sample is retained by the user on a token, say, a smart card⁸).

**Deployment Experience to Date**

The reality is that the highly lauded use of privacy-enhanced one-to-one biometric authentication technologies has simply not been widespread. Perhaps the best-known example has been its deployment in laptop computers, where users must match their biometric (fingerprint) in order to gain access to the laptop.

Public sector government bodies, on the other hand, have tended to insist on building large-scale interoperable biometric databases. The reasons for this preference are complex and worthy of exploration in a separate research paper. Briefly, however, some possible explanations are as follows:

- The claim of overriding public interests or (secondary) purposes that override individual privacy interests. It is here that the “zero-sum” game mentality prevails, i.e., more individual privacy equals less public security, and vice versa;

---


⁷ See Appendix 1 for documents and sources.

⁸ In the “real” world, the template or biometric image would be stored in a database as a backup in case the user lost his or her card. Otherwise, users would have to re-enroll every time they misplaced or lost their token. However, these databases would be limited and not networked, and encrypted.
Privacy by Design

- Unwillingness of system designers and operators to relinquish control over biometrics to individual users. Here, too, adding privacy is often viewed as compromising system functionality, control, and effectiveness;

- Requirements to carry out more and more background checks (e.g., against criminal records, terrorist watch lists, etc.) or to prevent multiple identity registrations and benefits fraud (welfare, medicare, driver's licences, immigration applications, etc.);

- Need to retain evidence and to make a criminal case when necessary (only biometric images verified by a human expert are accepted by courts, not just templates);

- Backup needs and escrow requirements – copies of biometric data need to be retained on file and made available to system operators and other authorities “just in case” the system fails;

- Unavailability of suitable, reliable, and cost-efficient privacy-enhanced biometric technologies and systems;

- Unreliable biometric enrolment/verification procedures and practices, which undermine ALL biometric systems if attackers can fraudulently impersonate others;

- Strong pressure from technology vendors and/or advice from independent consultants and integrators who may lack incentives to pursue privacy-enhanced biometric system options;

- The simplistic conflation of privacy and security, i.e., the misguided (and erroneous) belief that all biometric privacy interests can be satisfied by building system controls that seek to ensure confidentiality and integrity of the biometric data. This is a very common problem among security professionals, who tend to undervalue privacy as a separate and unique set of design principles; and

- Weak public demand and guidance from the privacy and data protection communities.

The reader will note that most of these explanations are predicated on zero-sum game thinking, i.e., more individual privacy and user control equals less of virtually everything else! Taken from this view, building true biometric privacy into an information system is invariably seen as a cost, rarely as an enhancement.

A more common deployment scenario is to carry out one-to-one biometric authentication against a single stored sample in a database. For example, a biometric-enabled identity card may have a serial number that acts as an index or lookup
Biometric Encryption: A Positive-Sum Technology That Achieves Strong Authentication, Security, and Privacy

key to the database, calling up the biometric “password” for one-to-one comparison and authentication against a live sample.

**Security Vulnerabilities of a Biometric System**

Biometric systems, especially one-to-one, may become vulnerable to potential attacks.9

Some of those security vulnerabilities include the following:

- **Spoofing.** It has been demonstrated that a biometric system can sometimes be fooled by applying fake fingerprints, face or iris image, etc.

- **Replay attacks,** e.g., circumventing the sensor by injecting a recorded image in the system input – much easier than attacking the sensor.

- **Substitution attack.** The biometric template must be stored to allow user verification. If an attacker gets an access to the storage, either local or remote, he can overwrite the legitimate user’s template with his/her own – in essence, stealing their identity.

- **Tampering.** Feature sets on verification or in the templates can be modified in order to obtain a high verification score, no matter which image is presented to the system.

- **Masquerade attack.** It was demonstrated10 that a digital “artefact” image can be created from a fingerprint template, so that this artefact, if submitted to the system, will produce a match. The artefact may not even resemble the original image. This attack poses a real threat to the remote authentication systems (e.g., via the Web), since an attacker does not even have to bother to acquire a genuine biometric sample. All he needs is just to gain an access to the templates stored on a remote server (this perfectly fits a description of a typical hacker operating from a rat hole).

- **Trojan horse attacks.** Some parts of the system, e.g., a matcher, can be replaced by a Trojan horse program that always outputs high verification scores.

- **Overriding Yes/No response.** An inherent flaw of existing biometric systems is due to the fact that the output of the system is always a binary Yes/No (i.e., match/no match) response. In other words, there is a fundamental disconnect between the biometric and applications, which makes the system open to potential attacks. For example, if an attacker were able to interject a false Yes response at a proper point of the communication between the biometrics and the

---


Figure 1: Privacy and security issues involving a biometric system
Biometric Encryption: A Positive-Sum Technology That Achieves Strong Authentication, Security, and Privacy

application, he could pose as a legitimate user to any of the applications, thus bypassing the biometric part.

- **Insufficient accuracy of many commercial biometric systems**, both in terms of FRR and FAR. High FRR causes inconvenience for legitimate users and prompts the system administrator to lower a verification threshold. This inevitably gives rise to FAR, which, in turn, lowers the security level of the system.

The privacy and security issues of a biometric system outlined in this section are illustrated in Fig. 1.

An enrolment part of any conventional biometric system consists of at least three blocks: a biometric sensor that acquires an image, a feature extractor that creates a biometric template, and a storage for the templates or images, or both. The storage can be either a database or a distributed medium.

A verification or identification part contains (at a minimum) a sensor to acquire a new image sample, and a matcher, which compares the image with the previously enrolled template(s) received from the storage. The output of the matcher is a Yes/No (i.e., match/no match) response that may go to the variety of applications.

A user of the system faces several privacy issues immediately at enrolment:

- Transparency, i.e., if the purpose of the system is clear to the user;
- If the enrolment is voluntary, and what the consequences are of not getting enrolled (for a variety of reasons);
- If the system can be trusted, i.e., if the personal data are adequately protected;
- Quality of biometric data: poor quality may lead to higher FRR and FAR. While FAR increases security risks for the system, a false rejection often causes some follow-up procedures, which can be privacy-invasive to the individual.

Other privacy/security issues were explained in the foregoing sections.
Biometric Encryption

Biometrics and Cryptography

Conventional cryptography uses encryption keys, which are just bit strings long enough, usually 128 bit or more. These keys, either “symmetric,” “public,” or “private,” are an essential part of any cryptosystem, for example, Public Key Infrastructure (PKI). A person cannot memorize such a long random key, so that the key is generated, after several steps, from a password or a PIN that can be memorized. The password management is the weakest point of any cryptosystem, as the password can be guessed, found with a brute force search, or stolen by an attacker.

On the other hand, biometrics provide a person with unique characteristics which are always there. Can they be used as a cryptographic key? Unfortunately, the answer is negative: biometric images or templates are variable by nature, i.e., each new biometric sample is always different. Conventional cryptography does not tolerate a single bit error.

As noted in the previous section, a biometric system always produces a Yes/No response, which is essentially one bit of information. Therefore, an obvious role of biometrics in the conventional cryptosystem is just password management, as mentioned by Bruce Schneier. Upon receiving a Yes response, the system unlocks a password or a key. The key must be stored in a secure location (so-called “trusted” device). This scheme is still prone to the security vulnerabilities noted in Fig. 1, since the biometric system and the application are connected via one bit only.

Biometric templates or images stored in a database can be encrypted by conventional cryptographic means. This would improve the level of system security, since an attacker must gain the access to the encryption keys first. However, most privacy issues associated with a large database remain, since the keys and, therefore, the biometric data are controlled by a custodian.

A comprehensive review of the issues involving biometrics and cryptography can be found elsewhere.

12 There has been recent activity of the International Organization for Standardization in order to support the confidentiality and integrity of the biometric template by using cryptographic means (ISO/IEC WD 24745, “Biometric Template Protection”):
www.fidis.net/fileadmin/fidis/deliverables/fidiswp3del3.2.study_on_PKI_and_biometrics.pdf
What Is Biometric Encryption?

Because of its variability, the biometric image or template itself cannot serve as a cryptographic key. However, the amount of information contained in a biometric image is quite large: for example, a typical image of 300x400 pixel size, encoded with eight bits per pixel has $300 \times 400 \times 8 = 960,000$ bits of information. Of course, this information is highly redundant. One can ask a question: Is it possible to consistently extract a relatively small number of bits, say 128, out of these 960,000 bits? Or, is it possible to bind a 128-bit key to the biometric information so that the key could be consistently regenerated? While the answer to the first question is problematic, the second question has given rise to the new area of research, called Biometric Encryption (BE).\(^{14}\)

Biometric Encryption is a process that securely binds a PIN or a cryptographic key to a biometric so that neither the key nor the biometric can be retrieved from the stored template. The key is recreated only if the correct live biometric sample is presented on verification.

“In Biometric Encryption, you can use the biometric to encrypt a PIN, a password, or an alphanumeric string for numerous applications – to gain access to computers, bank machines, to enter buildings, etc. The PINs can be 100s of digits in length; the length doesn’t matter because you don’t need to remember it. And most importantly, all one has to store in a database is the biometrically encrypted PIN or password, not the biometric template.”

Dr. George Tomko, OECD Report on Biometric-Based Technologies (2004)\(^{15}\)

The digital key (password, PIN, etc.) is randomly generated on enrolment so that the user (or anybody else) does not even know it. The key itself is completely independent of biometrics and, therefore, can always be changed or updated. After a biometric sample is acquired, the BE algorithm securely and consistently binds the key to the biometric to create a protected BE template, also called “private template.” In essence, the key is encrypted with the biometric. The BE template provides excellent privacy protection and can be stored either in a database or locally (smart card, token, laptop, cellphone, etc.). At the end of the enrolment, both the key and the biometric are discarded.

\(^{14}\) Other terms used for this technology: biometric cryptosystem, private template, fuzzy commitment scheme, fuzzy vault, fuzzy extractor, secure sketch, biometric locking, biometric key binding, biometric key generation, virtual PIN, biometrically hardened passwords, biometric signature, bioHashing. We use the term “Biometric Encryption” in a broad sense.

Privacy by Design

On verification, the user presents her fresh biometric sample, which, when applied to the legitimate BE template, will let the BE algorithm retrieve the same key/password. In other words, the biometric serves as a decryption key. At the end of verification, the biometric sample is discarded once again. The BE algorithm is designed to account for acceptable variations in the input biometric. On the other hand, an attacker, whose biometric sample is different enough, will not be able to retrieve the password. This encryption/decryption scheme is fuzzy, as the biometric sample is different each time, unlike an encryption key in conventional cryptography. Of course, it is a big technological challenge to make the system work.

After the digital key, password, PIN, etc., is retrieved, it can be used as the basis for any physical or logical application. The most obvious way lies in the conventional cryptosystem, such as a PKI, where the password will generate a pair of Public and Private keys.

Thus, Biometric Encryption is an effective, secure, and privacy-friendly tool for biometric password management, since the biometric and the password are bound on a fundamental level.

Advantages of Biometric Encryption (over Other Biometric Systems)

Biometric Encryption technologies have enormous potential to enhance privacy and security. Some of the key benefits and advantages of this technology include:

1. **No retention of the biometric image or template**
   From a privacy perspective, the best practice is not to collect any personally identifiable information (PII) at all in the first place, to the fullest extent possible. This is referred to as “data minimization” – minimizing the amount of personal data collected and retained, thus eliminating the possibility of subsequent abuse.
   
   Most privacy and security concerns derive from storage and misuse of the biometric data.
   
   A common concern is that “if you build it [the database], they will come [for the data].” The topline privacy and security concerns include fears of potential data matching, surveillance, profiling, interception, data security breaches, and identity theft by others. Misuse and mismanagement of biometric data by others invokes “negative externalities” and costs that fall primarily upon individuals rather than the collecting organization, but also at stake is the accountability and credibility of the collecting organization, and with them, the viability of the entire program.

   Biometric Encryption directly addresses these risks, threats and concerns.

   Users retain complete (local) control and use of their own biometrics.
Local control enhances confidence and trust in the system, which ultimately promotes greater enrolment and use.

2 Multiple/cancellable/revocable identifiers

Biometric Encryption allows individuals to use a single biometric for multiple accounts and purposes without fear that these separate identifiers or uses will be linked together by a single biometric image or template.

Thus, if a single account identifier becomes compromised, there is far less risk that all the other accounts will also be compromised.

Even better, Biometric Encryption technologies make possible the ability to change or recompute account identifiers. That is, identifiers may be revoked or cancelled, and substituted for newly generated ones calculated from the same biometric.

Traditional biometric systems simply cannot do this.

3 Improved authentication security: stronger binding of user biometric and identifier

Account identifiers are bound with the biometric and recomputed directly from it on verification. This results in much stronger account identifiers (passwords) because:

- they are longer and more complex;
- there is no need for user memorization; and
- they are less susceptible to security attacks.

Many security vulnerabilities of a biometric system listed in Fig. 1 are addressed:

No substitution attack: An attacker cannot create his own template since he, or anybody else, does not know the digital key and other transitory data that had been used to create the legitimate template;

No tampering: Since the extracted features are not stored, the attacker has no way to modify them;

No masquerade attack: Again, the system does not store the biometric template, so the attacker cannot create a digital artefact to submit to the system. Biometric Encryption provides an effective protection for remote authentication systems;

No Trojan horse attacks: BE algorithm does not use any score, either final or intermediate, to make a decision; it just retrieves (or does not retrieve) a key. Therefore, the attacker has no means to fool the system by outputting a high score;

No overriding Yes/No response: The output of BE algorithm is a 128-bit (or longer) digital key, as opposed to the binary Yes/No response. The attacker cannot obtain the key from a private template.
The security of Biometric Encryption technology can be augmented by the use of tokens (e.g., smart cards, PDA) and additional PINs, if needed.

4 Improved security of personal data and communications
As an added bonus, users can take advantage of the convenience and ease of Biometric Encryption technologies to encrypt their own personal or sensitive data. See Case Study #1 for an example.

Since the key is one’s own biometric, used locally, this technology could place a powerful tool directly in the hands of individuals.

Biometric Encryption could be viewed as encryption for the masses, made easy!

5 Greater public confidence, acceptance, and use; greater compliance with privacy laws
Public confidence and trust are necessary ingredients for the success of any biometric system deployment. One major data breach or horror story involving a large centralized database of biometric templates could set back the entire industry for years.

Data governance policies and procedures can only go so far to foster public trust. However, if privacy, security, and trust can be built directly into the biometric system, then the public and data protection authorities are far more likely to accept the privacy claims being made.

Putting biometric data firmly under the exclusive control of the individual, in a way that benefits that individual and minimizes risk of surveillance and identity theft, will go a long way toward satisfying the requirements of privacy and data protection laws, and will promote broader acceptance and use of biometrics.

6 Suitable for large-scale applications
Biometric Encryption technologies speak directly to the clear preference and recommendations of the privacy and data protection authorities for using biometrics to authenticate or verify identity, rather than for identification purposes alone.

Therefore, we prefer seeing biometrics used to positively link the bearer to a card or token, and to avoid creating systems that rely upon centralized storage and remote access/lookup of biometric data.

A prevailing reason for this view is that it is not known if biometric technology is sufficiently accurate and reliable to permit real-time identification in large $n$ samples, where $n$ is of an order of several million or higher. Despite these views, many large-scale one-to-many public biometric projects are being proposed and are well underway.
Often the biometric data in these systems are actually used for authentication purposes and not identification, but the lines between these two concepts can be blurred when multiple data items are collected and transmitted to a database for comparison. What becomes the identifier and what becomes the authenticator is somewhat arbitrary.

From a privacy point of view, transmitting biometric image or template data to a central database to be authenticated is risky enough without compounding the risks by sending more and more personal identifiers with it. “Multimodal” biometric solutions depend on collecting and comparing more than one biometric. It should be noted that the main reason for using “multimodal” solutions, besides providing a fallback for problem users, is insufficient accuracy/speed/security of existing biometrics. So the technical “solution” to using biometrics for authentication seems to be to collect more and more biometric and other personal data.

In 2006, the European Data Protection Supervisor (EDPS), Peter Hustinx, warned, in a formal opinion, of the privacy dangers of using biometric images or templates as an index or key to interoperable databases.16

Fortunately, Biometric Encryption technologies make possible database applications (see Case Study #3 as an example), minimizing the risks of traditional biometric systems (although we still prefer one-to-one applications with local template storage). It is possible to create secure and local biometric-enabled bindings of users to some other token identifiers without the need to reveal the actual biometric image or data.

It is further possible to create a so-called “anonymous database,” where a link between an anonymous identifier and encrypted (by conventional cryptographic means) user’s record is controlled by a Biometric Encryption process. This is very useful for a database containing sensitive information, such as medical records (see Case Study #2 for more details).

Another promising application of BE is a privacy-protected one-to-many database for “double dipping” prevention. The database is multimodal: it contains conventional but anonymous templates for one biometric (e.g., fingerprints) and private templates (e.g., for iris) that control a link with the user’s encrypted records. A user’s record would only be decrypted and displayed if there was a positive match on both conventional and private templates. Otherwise, all the information is inaccessible even to the system administrator.

16 See Appendix 1 for references and URLs.
With Biometric Encryption, users would be empowered by the ability to securely prove who they are to anyone, for any purpose, using their own biometrics, but without having to disclose the biometric data itself!

A high-level diagram of a Biometric Encryption process is shown in Fig. 2 (next page).

An enrolment part of a Biometric Encryption system consists of at least four blocks: a biometric sensor, a key generator that normally outputs a random key, a binding algorithm that creates a BE (private) template, and a storage for the BE template. Neither the key nor the image can be recovered from the BE template. The key, the image, and some transitory data are discarded at the end of the enrolment process.

A verification part contains at least a sensor to acquire a new image sample, and a key retrieval algorithm, which applies the image to the previously enrolled BE template received from the storage. The algorithm either retrieves the key, if the image on verification is close enough to the one enrolled, or fails to do so, in which case the user is rejected. The key enters an application, such as a PKI. Each application has its unique key. The biometric image is discarded at the end of the verification process.
Biometric Encryption: A Positive-Sum Technology That Achieves Strong Authentication, Security, and Privacy

Figure 2: High-level diagram of a Biometric Encryption process

Key generator

Sensor → Binding → Storage

Discard image, key

Reject

Sensor → Key retrieval

No key → Key → Application

Discard image
Current State of Biometric Encryption

The original concept of Biometric Encryption for fingerprints was pioneered in 1994 by Dr. George Tomko, founder of Mytec Technologies (Toronto, Canada). Since then, many research groups have taken part in the development of BE and related technologies. There are about 50 articles and patents published to date, most of which have appeared since 2002. The list of publications, with a brief review, is presented in Appendix 2.

Besides Biometric Encryption (BE), other terms have been used for this technology, such as: biometric cryptosystem, private template, fuzzy commitment scheme, fuzzy vault, fuzzy extractor, secure sketch, biometric locking, biometric key binding, biometric key generation, virtual PIN, biometrically hardened passwords, biometric signature, and bioHashing.

BE and related technologies have drawn attention from major academic research centres specializing in biometrics, such as Michigan State University, West Virginia University, Carnegie Mellon University, University of Cambridge (U.K.), and University of Bologna (Italy). Among current industry leaders, those worth noting include IBM T.J. Watson Research Center, RSA Laboratories, Lucent Technologies, Sandia National Laboratories, and Philips Research.

Virtually all types of biometrics have been tested to bind (or to generate) a digital key: fingerprints, iris, face, keystroke dynamics, voice, handwritten signatures, palm prints, acoustic ear recognition. The most promising results have been achieved with an iris: FRR = 0.47%, FAR = 0 (or at least less than one in 200,000) to generate a 140-bit key. These error rates are only marginally larger than for a conventional iris-based biometric system with the same input images17. The use of fingerprints is also feasible in terms of accuracy for BE, with FRR greater than 10% at present. Unlike an iris, there is a noticeable degradation in accuracy from a conventional fingerprint system. This is understandable since fingerprints are more prone to distortions and other factors that degrade accuracy. It is more difficult to compensate those factors in the case of Biometric Encryption, since BE works in a "blind" mode (the enrolled fingerprint or its minutiae template are not seen). There are several ways to overcome this problem, for example, by using a free air (i.e., contactless) fingerprint sensor, or by using more than one finger from the same person, or by combining several biometrics.18

Face recognition, which is usually considered third (after irises and fingerprints) in terms of accuracy in conventional biometrics, has shown a significant

17 The iris images were acquired in close to ideal conditions of a laboratory environment. In real life systems, some degradation of performance is expected, which is always the case with biometrics.

18 Note that even a 10% to 20% false rejection rate still may be acceptable for some applications with relatively low traffic and cooperative users: it simply means that a person would be rejected each fifth or tenth time on average and asked by the system to place the finger on the reader again.
Biometric Encryption: A Positive-Sum Technology That Achieves Strong Authentication, Security, and Privacy

improvement of performance over the last few years. This allowed Philips Research to create a working BE system using a face biometric. The published results range from FRR = 3.5% for a face database with low to medium variability of images to FRR = 35% for a database with high variability; FAR = 0 (or at least less than 1 in 100,000) in both cases. The key size used is 58 bits, which may be sufficient as a password replacement. According to communication from Dr. Michiel van der Veen of Philips Research, their technology, called privID™, is now operational and ready for deployment; in particular, it will be a part of a EU 3D Face project (WP2.5)\textsuperscript{19}. To the best of our knowledge, the Philips system will be the first real-life application of BE technology.

It is not clear if other biometrics have enough entropy (i.e., the amount of non-redundant information) in order to bind a sufficiently long key (e.g., 128 bit). This is an area of future research.

Some works published since 2002 provide a general theoretical foundation for BE technologies from a cryptographic point of view. They prove that the system can be made secure against “brute force” search attacks. In other words, an attacker checks at random all possible combinations in order to retrieve a key (or a biometric). Like conventional cryptography, it is assumed that the attacker is fully familiar with the algorithm, and may have a template in hand, but does not have a proper biometric to unlock the secret (i.e., the key bound to the biometric).

However, the attacker may try more sophisticated attacks, exploiting inherent weaknesses (if any) of the BE system and biometrics in general. This area of research has been largely overlooked. If such an attack is successful, the effective security of the system would be reduced from 128 bits to, perhaps, 69, 44, or an even lower number of bits. “This may seem an alarmingly small number to the crypto purist” (Hao, Anderson, and Daugman, 2005). On the other hand, BE is not just another cryptographic algorithm; it is rather a key/password management scheme. Key management has always been the weakest part of any cryptosystem, as it relies on passwords that may be forgotten, stolen, guessed, shared, etc. Biometric Encryption binds the key/password with the biometric and, thus, makes the system more secure. By comparison, a conventional biometric has only 1-bit security – a Yes/No response!

It is interesting to note that code-breaking becomes reduced to a security problem, not a privacy issue with BE, e.g., with an encrypted database of templates, breaking the encryption key exposes all the templates, and one has both a security and a privacy issue. Breaking a biometrically encrypted key, however, only exposes that key, but not necessarily the biometric, let alone the entire database, making it a far more secure system.

\textsuperscript{19} www.3Dface.org
With the notable exception of Philips privID™, to the best of our knowledge, there is no other commercially available BE system being used to date. The reason for this lies in both the technological challenges and existing market conditions. Not only the general public, but most high-tech developers are unaware of this emerging technology. Consequently, resources and funding in this area have, to date, been quite poor. We believe that the technological challenges have largely been overcome using an iris or face, and partially for fingerprints, bringing BE technology very close to the prototype development stage, and could soon be ready for testing in pilot projects.

Related Technologies
1. Storing a key in a trusted system
There have been some products\textsuperscript{20} that store a cryptographic key or a PIN in a so-called trusted system (e.g., a computer or a Digital Signal Processor (DSP)). The key is released upon successful biometric verification and then enters a conventional cryptosystem, e.g., Public Key Infrastructure (PKI). The biometric template (or image) is also stored somewhere, often in encrypted (by conventional means) form. If properly implemented, such systems may offer some security benefits. However, most problems outlined in the foregoing sections remain. For example, a binary Yes/No response is still required to release the key – this part of the algorithm is just hidden better. Most privacy issues associated with the template storage are also there.

Note that these systems often use the same terminology and/or claim the same benefits as BE, while in fact they do not provide a true binding between a key and a biometric.

2. Cancellable biometrics
A new area of research, closely related to BE, is called cancellable biometrics. It has been developed by IBM T.J. Watson Research Center, and by some academic groups. In this privacy-protecting technology, a distortion transform (preferably, irreversible) is applied to a biometric template. Only those distorted templates are stored, and they are matched also in the distorted form. If a distorted template is compromised, it can be “cancelled” by choosing just another distortion transform (i.e., the biometric is not lost). The transforms are application dependent, meaning that the templates cannot be reused by another applications (function creep is prevented).

\textsuperscript{20} See, for example:
Cancellable biometrics shares some other similarities with BE; for example, a technique called bioHashing can be used for both technologies. Unlike BE, a key is not generated or released in cancellable biometrics, so the system still produces a binary Yes/No response and is more vulnerable to attacks. The distortion transform should be truly irreversible (i.e., one way only) and kept secret. Otherwise, an attacker can either reconstruct the original biometric or create his own impostor template for a substitution attack, or even create an “artefact” image for a masquerade attack. Since the key is not generated, the variety of potential applications is narrower than for BE; for example, an anonymous database cannot be created. On the other hand, BE possesses all the functionality of cancellable biometrics, and, therefore, is a method for cancellable biometrics. Both technologies face similar accuracy/security challenges.

3. Fuzzy Identity Based Encryption
Another related technology, called Fuzzy Identity Based Encryption (FIBE), was proposed by A. Sahai and B. Waters in 2005. This technology also combines biometrics and cryptography on a fundamental level. Unlike BE, the user’s biometric is made somewhat public. In an example provided by D. Nali, C. Adams and A. Miri (see also a webcast presentation by B. Waters), a user (A) could go to a Driver Licensing Agency (D) and identify herself via an iris scan, under the ongoing surveillance of a trained agent. D could then use this scan to encrypt A’s information (e.g., an annual driver’s licence), when this information needs to be securely sent to A (e.g., via the Web). In order to obtain her biometric private keys, A would have to go in person to a trusted third party (e.g., a state agency), which would deliver keys via the same authenticating procedure as that used by D. A could then decrypt the message addressed to her using FIBE. She does not need a biometric reading at that point. In other words, A leaves her biometrics in at least two places, D and the trusted third party (often called Trusted Authority (TA)).

This scheme prevents impersonation of A by surreptitiously capturing her biometric sample, such as an iris photograph or latent fingerprints. “FIBE allows biometric measurements to be public” (Nali, Adams, and Miri) and, therefore, those surreptitious samples would become useless. While interesting from a scientific point of view, this technology is not privacy protecting, at least in the sense adopted by the privacy community (biometric data are considered personal information). There are also problems in handling a false rejection: user A may not have a chance to present another biometric sample if the false rejection occurs during decryption.

Scientific, Technological, and Privacy-Related Merits

Encryption with a fuzzy key (such as a biometric) was only recently introduced in conventional cryptography. Beyond such trivial things like accepting a few spelling errors in a password, or letting Alice partially share a list of her favourite movies with Bob, Biometric Encryption technologies are by far the most important application of those theoretical works. Market demand for such a technology would provide a great incentive to this promising area of modern mathematics and cryptography.

BE results in tougher requirements for distortion tolerance, discrimination, and the security of a biometric system. Solving these problems would be a significant scientific breakthrough both in the area of biometrics and cryptography. This would accelerate research and development of better biometric sensors and other hardware, as well as new, more accurate algorithms and software. No doubt this would bring technological benefits for the entire biometrics.

BE overcomes many security vulnerabilities of a biometric system, especially in a distributed environment. This could facilitate deployment of biometric systems on portable and handheld devices (laptops, cellphones, PDAs, etc.).

It would not be an overstatement to say that biometrics is perceived, in general, as a privacy-invasive technology. As we have shown, this perception is not baseless. Biometric Encryption, on the other hand, is a privacy-enhancing technology. It allows a user to retain full control over her biometric and, at the same time, to stay anonymous in many applications, i.e., to be represented only by a randomly generated (and cancellable) identifier linked to her biometric. No other personal data, e.g., address, telephone, date of birth, have to be revealed.

BE can render databases privacy protected, as they will comprise “private templates.” While such databases cannot be used for a background check, they are perfectly suitable for one-to-one access control systems or even for systems to prevent multiple registrations and related fraud. The user regains control over his or her sensitive information, such as medical or financial records, stored in the database.

Proliferation of BE technology may ultimately change the public’s perception of biometrics. This would raise the benchmark for biometric technologies, such that the industry would be prompted to develop and adopt new privacy-friendly solutions. If the “private templates” generated by BE make a significant presence in the market, this could reshape the entire biometric industry. Increased user acceptance and confidence would be extremely beneficial for the industry.
Case Study #1: Small-scale use of Biometric Encryption

To demonstrate the power of BE, we will briefly present a biometric authentication protocol (remote or local) with third party certification. We use a simplified and reworded description from Boyen’s paper on Fuzzy Extractors.22

Suppose that Alice wishes to authenticate herself to Bob using biometrics. Due to privacy concerns, she does not wish to reveal any biometric information to Bob. Conversely, for the authentication to be meaningful, Bob wants some assurance that Alice is in fact in possession of her purported biometrics at the time the authentication is taking place (i.e., that no one is impersonating her). We assume that there is a third party (often called the Trusted Authority), Trent, whom Bob trusts to honestly certify Alice’s biometrics, and to whom Alice will temporarily grant access to her biometrics for the purpose of generating such a certificate. Alice will want to be able to obtain as many or as few of those certificates as she wants, and to reuse as many of them with multiple Bobs, some of whom may be even dishonest, without fear of privacy leaks or risk of impersonation. The protocol is as follows:

Enrolment and certification: Under Trent’s supervision, and using Alice’s own biometric:

1. Alice creates a Biometric Encryption template from her biometric and a randomly selected PIN. Neither the biometric nor the PIN can be recovered from the template;
2. The PIN is used to generate a pair of keys, called public and private keys;
3. The biometric, the PIN, and the private key are discarded;
4. If Trent is satisfied that Alice has executed the steps honestly, he certifies the binding between Alice’s name and the public key, i.e., he digitally signs the pair [“Alice,” public key]. At this point, Alice may send the public key to Bob, or even publish it for all to see.

Verification: A challenge/response scheme is used to verify Alice:

1. At any time when appropriate (e.g., whenever Alice desires to authenticate herself to Bob), Bob sends Alice a fresh random challenge;
2. By obtaining her new biometric sample and applying it to her Biometric Encryption template, Alice recovers on-the-fly her PIN, which, in turn, regenerates her private key;
3. Alice signs the challenge with her private key and gives Bob the signature;
4. Bob authenticates Alice by checking the validity of the signature under her authentic public key.

The protocol does not require Alice to remember or store her PIN or her private key.

Privacy by Design

The Biometric Encryption template may be stored on a smart card or in Alice’s laptop, which also has a biometric sensor. For different applications (“multiple Bobs”), a new pair of public and private keys is generated from the PIN. Those keys are periodically updated. Some applications may require different PINs, in which case several Biometric Encryption templates can be stored. A proper template can be automatically recognized by the application.

The system based on digital signatures may be adopted both for a remote and local access. The important point is that the most critical part of any cryptosystem, the PIN (or a password), is securely bound to the biometrics.

In summary, Alice has in her possession and under her control as many BE templates as necessary. She can use them to digitally sign in, either for remote authentication or for logical or physical access. The authentication is done simply by checking the validity of her digital signature using standard cryptographic means. Neither Alice’s biometric nor her PIN is stored or revealed. As a result, the system is both secure and highly privacy protective.

Case Study #2: Anonymous database; large or medium-scale applications

Suppose that a clinic, a hospital, or a network of hospitals maintains a database of medical records. Alice does not want her record to be accessed by unauthorized personnel or third parties, even for statistical purposes. For that the latter, her record is made anonymous and encrypted (by conventional means). The only public entry in the database is her personal identifier, which may be her real name or, in certain cases (e.g., drug addiction clinic), an alias (“Jane Doe”). The link between Alice’s identifier and her medical record is controlled by Biometric Encryption:

On enrolment, a BE template is created from Alice’s biometric and a randomly generated PIN (Alice does not even know the PIN). The PIN is used to generate a pointer to Alice’s medical record and a crypto-key that encrypts the record, and also a pair of keys called public and private keys (similar to Case Study #1). The BE template and the public key are associated with Alice’s ID and stored in the database (they can also be stored on Alice’s smart card); other temporary data, such as Alice’s biometric, the PIN, the private key, the pointer, and the crypto-key, are discarded.

Suppose that Alice visits a doctor, to whom she wants to grant remote access to her medical record, or part of it, if the record is structured. From the doctor’s office, Alice makes a request to the database administrator, Bob. The authentication procedure using challenge/response scheme is similar to that in Case Study #1:
Biometric Encryption: A Positive-Sum Technology That Achieves Strong Authentication, Security, and Privacy

1. If Alice does not have her smart card with her (e.g., in the case of an emergency), Bob sends Alice's BE template to the doctor's office;

2. Alice applies her new biometric sample to the BE template and recovers on-the-fly her PIN;

3. The PIN is used to regenerate her private key, the pointer to her medical record, and the crypto-key;

4. Bob sends Alice a fresh random challenge;

5. Alice signs the challenge with her private key and gives Bob the signature;

6. Bob authenticates Alice by checking the validity of the signature under her public key;

7. Alice securely sends Bob the pointer to her medical record;

8. Bob recovers Alice's encrypted medical record (or a part of it, also encrypted) and sends it to Alice;

9. Using her crypto-key, which was regenerated from her PIN, Alice decrypts her medical record for the doctor;

10. Alice's biometric, the PIN, the private key, the pointer, and the crypto-key, are discarded.

In summary, Bob (the database administrator) has an assurance that Alice is, in fact, who she claims to be (she was able to unlock her BE template in the doctor's office); he is also assured that her medical record was sent to the right person. On the other hand, Alice retains full control over her medical record, so that even Bob has no access to it, since he does not have the crypto-key to decrypt it. The privacy protection is embedded into the system at a very basic technological level.

Case Study #3: Travel documents; large-scale database applications

Using biometrics for travel documents has been a hot topic of discussion. To illustrate how BE can protect the user's privacy and, at the same time, improve the level of security, we will consider a reworded description of a system proposed by Dr. van der Veen et al. (Ref. [40] in Appendix 2).

The International Civil Aviation Organization (ICAO) dictates international standards for Machine Readable Travel Documents (MRTD), including those for ePassports. Among the recommendations is the “three-way-check” for secure verification at a border crossing. It involves comparing data originating from (i) the biometric sensor, (ii) the biometric image stored on the ePassport, and (iii) biometric data stored in external (centralized) databases.
BE technology provides the opportunity to do this in a privacy-preserving manner: in addition to the biometric templates stored on the ePassport, their secure versions, namely, the BE templates, are also stored in a third-party database. The biometric images or conventional templates are not stored in the database. A “three-way check” is then performed by matching the BE template from the database to that appearing on the ePassport, and the live biometric measurement scanned at the kiosk. Border passage now involves the following steps:

1. At a kiosk, a user claims his identity (ID), and presents his biometric (e.g., facial image, fingerprint or iris) for measurements;
2. The ID is sent to the third-party database to extract the corresponding BE template;
3. The BE template is transmitted to the kiosk;
4. The BE template and the biometric measurement are combined to derive a cryptographic key, or rather a hashed version of it;
5. The image of the iris, face or fingerprint is extracted from the ePassport and used together with the BE template to derive another hashed version of the cryptographic key. This will validate the biometric stored on the ePassport;
6. Both hashed versions of the key derived in Steps 4 and 5 are transmitted to the border-control authority and verified against the database version. A positive authentication is achieved when all three versions are exactly the same.

In summary, the user’s privacy is protected since the biometric image or template is not stored in a central database; instead, a secure BE template is stored. The database is inherently secure, meaning there is no need for complicated encryption and key management protocols. The ePassport is protected against tampering, since a potential attacker or any unauthorized user will not know the cryptographic key that was used to create the BE template.

Next Steps to Bringing Biometric Encryption to the Prototype Stage

Biometric Encryption has been researched since the mid-90s. Technologically, this area is much more challenging than conventional biometrics. But now BE is fast approaching the next phase, i.e., the creation and testing of a prototype. The following issues still need to be addressed:

Select a Proper Biometric

The most promising results in terms of accuracy have been obtained for irises. Low variability of image samples and the presence of a natural alignment feature (eye pupil) make this biometric the number one candidate for BE.
Face recognition is the most publicly acceptable type of biometric. Recent advances in the technology allowed Philips Research to create the first operational BE system. At the present time, one of the drawbacks of the face-based BE system, however, is the relatively small size (~58 bits) of the encryption key that may be securely bound to the biometric.

Fingerprints, for which the BE was originally pioneered, are also a prime choice. The fingerprint biometric is used more widely than the iris or face, and most privacy concerns relate to fingerprints. On the other hand, using fingerprints for BE turns out to be much more challenging. The reasons are: high skin distortions can be introduced when the finger presses upon the sensor; and the difficulty of aligning a fingerprint on verification with the one enrolled. As mentioned before, the situation is more difficult for BE than for a conventional fingerprint verification, since BE works in a “blind” mode (the enrolled fingerprint or its minutiae template are not seen). Some of these issues can be overcome with a free-air image. Although this would present other optical issues, we believe they could be resolved by current technology. In general, face and especially iris are less vulnerable to distortion and alignment problems.

Other biometrics, e.g., voice, signature, palm prints, etc., may not have enough entropy (i.e., the amount of non-redundant information to support a long enough cryptographic key). They could possibly be put on the list of “auxiliary” biometrics, i.e., used for BE in combination with irises, faces, or fingerprints or, perhaps, with conventional passwords (called “hardening”).

**Improve the Image Acquisition Process**

For fingerprints, this means choosing a proper fingerprint sensor that is less susceptible to skin distortions (e.g., a free air sensor), or changing the existing sensor ergonomics to keep the distortions under control. Image quality can also be improved at the algorithm level (i.e., through software).

**Make BE Resilient Against Attacks**

This area of research, i.e., the analysis of potential vulnerability of BE against attacks, has been largely overlooked. By that we mean that a sophisticated attacker could gain access to both the BE templates and the algorithm. The only thing he cannot obtain is a user’s biometric. Such an attacker, fully familiar with the algorithm and exploiting its weaknesses, will not be doing just a brute force search (i.e., about $2^{128}$ computations for a 128-bit key) in order to break the BE template. Instead, he will devise various attacks that can be run in a realistic time frame. The

23 There have been independent tests, such as BioPII in Germany, that reported unusually high error rates for iris recognition: [www.bsi.de/literat/studien/biop/biopabschluss2.pdf](http://www.bsi.de/literat/studien/biop/biopabschluss2.pdf); [www.europeanbiometrics.info/images/resources/90_264_file.pdf](http://www.europeanbiometrics.info/images/resources/90_264_file.pdf). Those results were questioned by Prof. John Daugman (“BioPII Controversy to Be Tackled,” *Biometric Technology Today*, vol. 13, no. 10, pp. 1-2, 2005).
BE algorithm must be resilient against those off-line attacks. The same approach (i.e., resilience against attacks) is adopted in conventional cryptography.

**Improve Accuracy and Security of BE Algorithm**

There have been substantial advances in algorithm development in conventional biometrics in the past few years, as demonstrated by a series of international competitions. Many of those advances are applicable to BE.

**Exploit Multimodal Approaches**

This has been a hot area of research and development in conventional biometrics. The performance of a biometric system is significantly improved when different algorithms, or different fingers, or different biometrics (e.g., fingerprints and face) are combined. The modes that are combined should be “orthogonal,” i.e., statistically independent. It is reasonable to expect that the multimodal approach would also work for BE.

**Develop BE Applications**

The applications, such as those described in the case studies, should clearly demonstrate the benefits for privacy and security brought about by the use of BE.

**Summary and Conclusions**

Biometric Encryption technology is a fruitful area for research and has become sufficiently mature for broader public policy consideration, prototype development, and consideration of applications.

This paper has explored the possibilities and privacy-enhancing benefits of Biometric Encryption technologies for meeting the needs of businesses and government agencies.

We believe that BE technology exemplifies fundamental privacy and data protection principles that are endorsed around the world, such as data minimization, user empowerment, and security, better than any other biometric technology solution in existence.

We hope that our paper will form a valuable contribution to current national and international discussions regarding the most appropriate methods to achieve, in a privacy-enhanced manner, strong identification and authentication protocols.

While introducing biometrics into information systems may result in considerable benefits, it can also introduce many new security and privacy vulnerabilities, risks, and concerns, as discussed above. However, novel Biometric Encryption techniques have been developed that can overcome many, if not most, of those risks and vulnerabilities, resulting in a win-win, positive-sum scenario.

One can only hope that the biometric portion of such systems is done well, and preferably not modelled on a zero-sum paradigm, where there must always be a winner and a loser. A positive-sum model, in the form of Biometric Encryption, presents distinct advantages to both security AND privacy.
Appendices

For the two extensive appendices, please see the online version of Biometric Encryption: A Positive-Sum Technology That Achieves Strong Authentication, Security, and Privacy at www.ipc.on.ca.

About the Authors

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner of Ontario Dr. Ann Cavoukian is recognized as one of the leading privacy experts in the world and is the author of two groundbreaking books on privacy – Who Knows: Safeguarding Your Privacy in a Networked World (1997), written with Don Tapscott, and The Privacy Payoff: How Successful Businesses Build Customer Trust (2002), written with Tyler Hamilton. Overseeing the operations of the access and privacy laws in Canada's most populous province, Commissioner Cavoukian serves as an Officer of the Legislature, independent of the government of the day.

Alex Stoianov, Ph.D.
Dr. Alex Stoianov began working in the field of biometrics after joining Mytec Technologies Inc. (Toronto, Canada) in 1994, where he was one of the originators of the privacy-enhancing technology Biometric Encryption. Working for Bioscrypt Inc., the successor of Mytec, as a Principal Scientist from 2001 to 2006, he developed numerous technological breakthroughs and improvements for fingerprint verification algorithms. He also won the Third International Fingerprint Verification Competition (FVC2004), viewed by many as the “Fingerprint Olympics,” on the company’s behalf. Dr. Stoianov has co-authored over 30 scientific papers and seven patents.

The authors gratefully acknowledge the work of Fred Carter, IPC Senior Policy and Technology Advisor, in the preparation of this paper.

The authors would also like to thank Prof. Dr. Christoph Busch of Fraunhofer IGD, Germany, and Mr. Bernard Didier and Mme. Alexandra Michy, both of Sagem Défense Sécurité, France, for their review and contributions to the pre-publication draft.

In addition, we would like to thank Dr. Michiel van der Veen, Senior Manager, Business Development Biometrics, Philips Research, of the Netherlands, for bringing to our attention their recent white paper, privID™: Privacy Protection in Biometric Security Applications, as well as the fact that Philips now has biometric encryption applications that are operational and ready for deployment.
Privacy Guidelines for RFID Information Systems
(RFID Privacy Guidelines)

June 2006
Privacy Guidelines for RFID Information Systems (RFID Privacy Guidelines)

Introduction

This document is intended to serve as privacy “best practices” guidance for organizations when designing and operating Radio-Frequency Identification (RFID) information technologies and systems.

The Information and Privacy Commissioner of Ontario (IPC) has a mandate to educate the public and address privacy questions raised by new information technologies, with a view to encouraging effective solutions. Accordingly, the IPC has developed these Guidelines in partnership with industry and other stakeholders. The Guidelines are not intended to supersede any applicable privacy law or regulation.

We recognize that RFID tags are becoming more prevalent in our everyday lives, and offer many benefits and conveniences, from security access cards to ignition immobilizers to highway toll systems and other electronic pass systems.

RFID tags deployed in the supply chain process pose little threat to privacy – they are not linked to any individual but rather, placed on crates, pallets and cases to track products. They act as a unique identifier that uses Radio Frequency Identification for the automatic identification of products in the supply chain. These tags contain standard information pertaining to the products and do not include any personal information.

In order to allow RFID technology to realize its potential for consumers, retailers and suppliers, it is vital that we address privacy concerns prompted by the current state of the technology, while establishing principles for dealing with its evolution and implementation. Accordingly, we encourage organizations to observe and adopt the Guidelines contained in this document whenever deploying RFID technology with consumer-facing implications.

The use of RFID tags in the supply chain management process is not the problem. The problem arises with their use at the consumer item-level. RFID tags, when linked to personally identifiable information, present the prospect of privacy-invasive practices relating to the tracking and surveillance of one’s activities. The goal of these Guidelines is to alleviate the privacy-related concerns associated with such data linkages, while increasing the openness and transparency associated with RFID systems. The use of these Guidelines will ultimately facilitate the preservation of trusted business relationships with existing customers, and perhaps assist in attracting new ones.
**Scope**

These RFID Privacy Guidelines apply to any organization that operates an information system involving the use of RFID technology on consumer products involving or potentially linking to, personally identifiable information.

“Organization” refers broadly to associations, businesses, charitable organizations, clubs, government bodies, institutions, and professional practices. In most instances, these Guidelines will be especially relevant to retailers.

“Information system” refers to any combination of RFID tags, readers, databases and networks that serve to collect, transmit, process and store RFID and RFID-linked information.

“Personal information” refers to any recorded information about an identifiable individual. In addition to one’s name, contact and biographical information, this could include information about individual preferences, transactional history, record of activities or travels, or any information derived from the above, such as a profile or score, and information about others that may be appended to an individual’s file, such as about family, friends, colleagues, etc. In the context of item-level RFID tags, the linkage of any personally identifiable information with an RFID tag would render the linked data as personal information.

These Guidelines are based upon the 10 principles of the 1996 Canadian Standards Association (CSA) Privacy Code, which were formulated by a wide range of stakeholders, including business, industry and consumer groups. The principles of the CSA Privacy Code now serve as the basis for Canadian privacy laws and regulations across Canada. They are observed by Canadian organizations in their day-to-day policies and practices, and are widely recognized as being one of the strongest and clearest expressions of privacy “fair information practices.”
The Guidelines and their application are informed by the following three overarching principles:

1) **Focus on RFID Information Systems, Not Technologies:** The problem does not lie with RFID technologies themselves; it is the way in which they are deployed that raise privacy concerns. For this reason, we prefer to speak broadly of RFID information systems. These Guidelines should be applied to RFID information systems as a whole, understood in their broader contexts, rather than to any single technology component or function.

2) **Privacy and Security Must Be Built in from the Outset – at the Design Stage:** Just as privacy concerns must be identified in a broad and systemic manner, so too must technological solutions be addressed systemically. A thorough privacy impact assessment is critical. Users of RFID technologies and information systems should address the privacy and security issues early in the design stages, with a particular emphasis on data minimization. This means that wherever possible, efforts should be made to minimize the identifiability, observability and linkability of RFID tags with personal information and other associated data.

3) **Maximal Individual Participation and Consent:** Use of RFID information systems should be open and transparent, and offer individuals as much opportunity as possible to participate and make informed decisions.

This document provides voluntary, consensus-based guidance that recognizes the great variety of uses and applications for RFID technologies and information systems. Because of this heterogeneity, a degree of flexibility in its interpretation and application may be necessary.

We encourage organizations to adopt and to adapt these Guidelines for use in their own policies, procedures and applications, according to their own specific circumstances and needs.
RFID Privacy Guidelines

1 Accountability
An organization is responsible for personal information under its control and should designate a person who will be accountable for the organization's compliance with the following principles, and the necessary training of all employees. Organizations should use contractual and other means to provide a comparable level of protection if the information is disclosed to third parties.

Organizations that typically have the most direct contact and primary relationship with the individual should bear the strongest responsibility for ensuring privacy and security, regardless of where the RFID-tagged items originate or end up in the product life cycle.

2 Identifying Purposes
Organizations should clearly identify and communicate to the individual the purposes for collecting, linking to, or allowing linkage to personal information, in a timely and effective manner. Those purposes should be specific and limited, and the organizations and persons collecting personal information should be able to explain them to the individual.

3 Consent
Organizations must seek individual consent prior to collecting, using, or disclosing personal information linked to an RFID tag. To be valid, consent must be based upon an informed understanding of the existence, type, locations, purposes and actions of the RFID technologies and information used by the organization. Individual privacy choices should be exercised in a timely, easy and effective way, without any coercion. Consumers should be able to remove, disable or deactivate item-level RFID tags, without penalty.

Automatic deactivation of RFID tags, at the point of sale, with the capability to re-activate, should be the ultimate goal. Consumers should be able to choose to re-activate them at a later date, re-purpose them, or otherwise exercise control over the manner in which the tags behave and interact with RFID readers.

4 Limiting Collection
Organizations should not collect or link an RFID tag to personally identifiable information indiscriminately or covertly, or through deception or misleading purposes. The information collected should be limited to the minimum needed to fulfill the stated purposes, with emphasis on minimizing the identifiability of any personal data linked to the tag, minimizing observability of RFID tags by unauthorized readers or persons, and minimizing the linkability of collected data to any personally identifiable information.
5 Limiting Use, Disclosure and Retention
Organizations must obtain additional individual consent to use, disclose or link to personal information for any new purposes. Personal information should only be retained to fulfil the stated purposes, and then securely destroyed. Retailers should incorporate the data minimization principles outlined above, into and throughout their RFID information systems.

6 Accuracy
Organizations should keep personal and related RFID-linked information as accurate, complete, and up-to-date as is needed for the stated purposes, especially when used to make decisions affecting the individual.

7 Safeguards
Organizations should protect personal information linked to RFID tags, appropriate to its sensitivity, against loss or theft, and against unauthorized interception, access, disclosure, copying, use, modification, or linkage. Organizations should make their employees aware of the importance of maintaining the confidentiality of personal information through appropriate training. Although physical, organizational and technological measures may all be necessary, technological safeguards should be given special emphasis.

8 Openness
Organizations should make readily available to individuals specific information about their policies and practices relating to the operation of RFID technologies and information systems, and to the management of personal information. This information should be made available in a form that is understandable to the individual.

9 Individual Access
Organizations should, upon request, inform the individual of the existence, use, linkage and disclosure of his or her personal information, provide reasonable access to that information, and the ability to challenge its accuracy and completeness, and have it amended as appropriate.

10 Challenging Compliance
Organizations should have procedures in place to allow an individual to file a complaint concerning compliance with any of the above principles, with the designated person accountable for the organization's compliance.
RFID and Privacy:
Guidance for Health-Care Providers

January 2008
RFID and Privacy:
Guidance for Health-Care Providers

Foreword

Health-care providers around the world are recognizing the benefits of adopting Radio Frequency Identification (RFID) technology into their operations, in order to enhance health care service delivery. The availability and use of innovative new RFID-enabled information technology applications are helping providers to track medical equipment and supplies more efficiently, verify the authenticity and administration of drugs, and improve patient safety and security, such as by using RFID-enabled identification bracelets for newborns and patients. However, as the benefits of RFID uses and applications are realized, concerns are also being raised about the potential privacy implications associated with use of this technology, especially when RFID tags are linked to identifiable people.

In the autumn of 2006, I was approached by Victor Garcia, Chief Technology Officer for Hewlett-Packard (HP) Canada, seeking the expertise of my office in how potential privacy issues could be identified and safeguards developed and implemented into the usage of RFID technology. I was more than willing to contribute my insight and expertise because, as Commissioner, part of my mandate includes reaching out to external organizations. I have also found it beneficial to assist both public and private organizations working on emerging technologies, and to always be proactive whenever possible – to develop effective guidelines and codes of conduct before any problems arise. Further, I was also interested in working with HP given that it is an organization that takes the protection of privacy very seriously, having a history of working alongside legislative and standards bodies, partners, customers, and NGOs to help drive the adoption of privacy principles to protect consumer privacy rights. Specifically regarding HP’s work with RFID, I was encouraged by its corporate values in that individuals should always be given notice about the presence of RFID tags, and where possible, have the choice to remove or deactivate RFID tags. HP products with an RFID tag on the box are always accompanied by an EPCglobal logo, which alerts the consumer to the presence of the tag. Lastly, I was also impressed by the fact that my colleagues at HP and I share the same belief – that being visible about RFID use will breed confidence in the technology, while being secretive will heighten the misconceptions and fears.

My work with RFID began in 2003 when I released Tag, You’re It: Privacy Implications of Radio Frequency Identification (RFID) Technology, and I first identified the potential privacy concerns raised by RFID technology. Since then, I have gone on to work with a number of organizations such as EPCglobal Canada, with whom I consulted when I wrote Privacy Guidelines for RFID Information Systems.
(RFID Guidelines). My office has also helped to shape policy and ideas, from RFID tags in Ontario’s public libraries to lectures on how to implement privacy protections in RFID systems. This publication is a continuation of my ongoing work with RFID. For many months, IPC and HP staff worked hard to examine questions regarding RFID privacy protections. The result is this co-authored document.

The essential purpose of this publication is to assist the health-care sector in understanding the current and potential applications of RFID technology, its potential benefits, its privacy implications, and steps that can be taken to mitigate potential threats to privacy. I, and my co-author, Victor Garcia at Hewlett-Packard, sincerely believe that this document will serve as a benchmark for considerations relevant to the application of, and the privacy issues associated with, RFID technology in health care.

During the time I was working toward making the Personal Health Information Protection Act (PHIPA) a reality, I repeatedly stated that, “I believe in the necessity of PHIPA not only because I am the Commissioner, but also because I am a patient.” I believe that the same sentiment also applies to this document. While I, as a patient, would welcome the prospect of RFID technology improving my health-care services, I, as Commissioner, also believe that we must ensure the deployment of this technology does not infringe upon our privacy.

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

About the Authors

Information and Privacy Commissioner of Ontario (IPC)
In her mandate and role in relation to personal health information, the Information and Privacy Commissioner of Ontario has the authority to oversee compliance with the Personal Health Information Protection Act (PHIPA). The Act authorizes the IPC to review complaints about a person who has contravened or is about to contravene PHIPA, and review complaints related to the right of individual access and correction. It also authorizes the IPC to engage in or to commission research into matters affecting PHIPA, conduct public education programs, and provide information on PHIPA and its role thereunder.

Hewlett-Packard (HP)
One of the world’s largest IT companies, Hewlett-Packard (HP) is not only involved in the development of innovative RFID technologies and applications, it is also committed to improving health care by focusing on: delivering solutions that allow health-care providers better access to patient information by integrating systems, data, processes and people; providing staff and patients with secure access to information, data and applications; and transforming business processes and IT to better serve the public interest.
Introduction

Information and communications technologies (ICTs) are transforming the world we live in through revolutionary developments in bandwidth, storage, processing, mobility, wireless, and networking technologies.

The health-care sector has recognized the value of new technology in the delivery of health care. For example, globally, billions of dollars are now spent annually on advanced diagnostic and treatment equipment. Until recently, however, ICTs were limited to administrative and financial applications and played only a small role in direct care for patients. But we are beginning to see an evolutionary – perhaps even revolutionary – change in how health care is delivered.

Health-care providers around the world are undergoing a digital transformation, harnessing cutting-edge IT to increase operational efficiencies and save lives. For example, they are replacing expensive, hard-to-share and easily lost X-ray films with digital images that can be effortlessly and securely shared, stored, transmitted and accessed. They are also moving away from an environment dominated by hand-written notes and physician orders to one where staff use ICTs to document patient records and enter and process orders. Thanks to ICTs, the vision of comprehensive and instantly available electronic health records is now within reach.

But the digital transformation is about much more than just software applications. It involves taking advantage of advanced technology such as RFID to imaginatively meet a host of needs. Invented over 60 years ago, RFID is fundamentally a technology for automatic identification that can be deployed in a nearly unlimited number of ways. The technology is starting to hit its stride, finding a wealth of new uses and applications related to automated identification, safety and business process improvement.

Patient safety is one of the most critical issues in the health-care sector today. There is a mounting concern about medical errors, such as from the administration of incorrect medications or dosages, or from patients being misidentified. A 1999 study of 1,116 hospitals by the United States Institute of Medicine suggests that more than 44,000 deaths occur each year in the United States as a result of in-hospital medication errors.1 Canadian estimates put the figure at 700 deaths per year due to medication errors.2 A 2002 study of medication errors at 14 acute-care hospitals in Ontario counted over 4,000 errors, only 800 of which were

---

counted as adverse drug effects. A similar study conducted at the Children’s Hospital of Eastern Ontario, published in 2003, counted over 800 medication errors during a six-year period. RFID technologies may offer remedies for these patient safety problems.

Operational inefficiencies, in some cases due to the inability to rapidly find and track medical equipment, are also a concern for the health-care sector. It has been estimated that the theft of equipment and supplies costs hospitals $4,000 per bed each year and with over 975,000 staffed beds in the U.S., this represents a potential loss of $3.9 billion annually. Considerable time and effort is spent searching for valuable mobile medical assets, and in maintaining an accurate and up-to-date inventory – human resources that might otherwise be better dedicated to more productive ends. Once again, RFID technologies can help provide cost-effective solutions.

Increasingly, there is considerable interest in exploring the uses of new technology to better understand processes, achieve greater operational efficiencies and improve patient safety.

In the health-care sector, RFID technology is already being used to rapidly locate medical equipment and devices, track surgical equipment, specimens and laboratory results, identify and verify the authenticity of pharmaceuticals (including for stock rotation and recalls), and to ensure that the right medicine, in the right dosage, is given to the right person at the right time. Other applications include positively identifying patients, prescribing and checking drug interactions at the point of care, quickly checking a patient’s blood type, matching newborn infants with their parents, and triggering a lock-down after the unauthorized removal of an infant from a secured area. Finally, RFID technology is being effectively used to help improve patient registration and management processes at hospitals, leading to analysis of bottlenecks, improvement in flow and reduction in wait times.


4 W. James King, MSc, MD*, Naomi Paice, MD*, Jagadish Rangrej, MMath, Gregory J. Forestell, MHA | I and Ron Swartz, BScPharm, The Effect of Computerized Physician Order Entry on Medication Errors and Adverse Drug Events in Pediatric Inpatients, in PEDIATRICS Vol. 112 No. 3 Sept 2003, pp. 506-509, at: http://pediatrics.aappublications.org/cgi/content/abstract/112/3/506


Pilot projects are underway in Canada. In January 2006, Hamilton Health Sciences, in conjunction with the RFID Applications Lab at McMaster University, launched a multi-phased multi-year RFID initiative to explore and assist in development of better business intelligence tools for health care. The initial effort was focused on exploring the economic and technical feasibility of using RFID to track valuable mobile assets in real-time. Expected efficiency benefits include labour savings, reduced capital expenditure for equipment, equipment and item loss prevention, and process improvements. Future phases of the project are aimed at looking at optimizing and improving processes related to daily operations such as asset management as well as patient care by using evolving technology as an enabler. These may include using RFID for patient identification and pandemic planning, depending on the results of their planned privacy study.

In January 2008, London (Ontario) Health Sciences commenced the first implementation phase of their RFID strategy, with an RFID pilot deployed by Hewlett-Packard designed to track infusion pumps and other critical medical equipment in real-time, providing business intelligence and operational data based on the location and utilization of equipment. London Health Sciences’ vision for the application of RFID within their facilities includes leveraging automatic identification and tracking systems to achieve better use of medical equipment, equipment and item loss prevention, and process improvements, eventually leading to increased patient safety in proper balance with privacy protection, confidentiality and data security.

Perhaps the most intensive use of RFID technology would be in a contagion research facility, where all people and items – and the interactions among them – can be closely tracked and monitored (some pandemic emergency scenarios also call for fine-grained location, tracking and audit capabilities). Perhaps the most innovative RFID technologies being developed today are biosensors – specialized RFID chips implanted into bodies to monitor and transmit critical health conditions.

These publicized applications of RFID technology in Canada and around the world have highlighted the potential for widespread use of this technology in the health-care sector. Factors prompting the publication of this document include:

- The increasing availability of RFID-based solutions for the health-care sector;
- The growing interest in the use of this technology by health-care providers; and
- The concerns that have been raised about the potential privacy implications associated with the use of RFID technology in the health-care sector.

This paper provides a balanced analysis of RFID technology by examining a wide variety of RFID applications in the health-care sector from around the world, and organizing them into three broad categories:
Privacy by Design

- RFID technology to track things;
- RFID technology to track things linked to people; and
- RFID technology to track people.

The paper also identifies the benefits and potential privacy issues associated with this technology and the steps that may be taken to mitigate the threat to privacy.

**What Is Privacy?**

**Informational privacy defined**

Informational privacy is the right of an individual to exercise control over the collection, use, disclosure and retention of his or her personal information, including his or her personal health information. Personal information (also known as personally identifiable information or “PII”) is any information, recorded or otherwise, relating to an identifiable individual. Almost any information, if linked to an identifiable individual, can become personal in nature, be it biographical, biological, genealogical, historical, transactional, locational, relational, computational, vocational, or reputational. The definition of personal information is quite broad in scope. The challenges for privacy and data protection are equally broad.

**How privacy is regulated in the health-care sector in Ontario**

On November 1, 2004, the *Personal Health Information Protection Act (PHIPA)*\(^6\) came into effect in the province of Ontario. *PHIPA* provides individuals with control over the collection, use and disclosure of their personal health information by requiring persons and organizations in the health sector, defined as health information custodians, to collect, use and disclose personal health information only with the consent of the individual to whom the information relates, subject to limited exceptions. It also provides individuals with the right to access and require correction of their personal health records, subject to specific exceptions.

*PHIPA* defines “personal health information” as identifying information about an individual that, among other things, relates to the physical or mental health of the individual, relates to the provision of health care to the individual, identifies a provider of health care to the individual, identifies the substitute decision-maker of the individual, or is the individual’s health number.

It defines a “health information custodian” as a person or organization listed in *PHIPA* that has custody or control of personal health information. Examples of health information custodians include health-care practitioners, hospitals, psychiatric facilities, long-term care homes, pharmacies, laboratories, and ambulance services.

---

\(^6\) *PHIPA* text available at: [www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm](http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm) and A Guide to the Personal Health Information Protection Act available at: [www.ipc.on.ca/images/Resources/hguide-e.pdf](http://www.ipc.on.ca/images/Resources/hguide-e.pdf)
PHIPA reflects worldwide privacy criteria, such as the principles of fair information practices set forth in the Canadian Standards Association Model Code for the Protection of Personal Information7 and the Global Privacy Standard, an effort of the international privacy and data protection commissioners, led by the IPC, to harmonize the various privacy codes and practices currently in use around the world.8

Obligations of the health-care sector in relation to personal health information

Health information custodians are required, under PHIPA, to collect, use and disclose personal health information only with the consent of the individual to whom the personal health information relates, subject to limited exceptions. They are also required to comply with the wishes of an individual who withholds or withdraws consent, or who gives express instructions that the information must not be used or disclosed for health-care purposes in certain circumstances.

PHIPA also prohibits health information custodians from collecting, using or disclosing personal health information if other information will serve the purpose and requires that only the information that is reasonably necessary be collected, used, or disclosed. Custodians are required to take reasonable steps to ensure that personal health information is protected against theft, loss and unauthorized use or disclosure, ensure that records are protected against unauthorized copying, modification and disposal, and retain, transfer, and dispose of health information in a secure manner.

In addition, PHIPA requires health information custodians to provide individuals with the right to access their records and have them corrected subject to specific exceptions.

Obligations of electronic services providers in relation to personal health information

Suppliers of electronic services (who are not agents) that enable the health information custodian to collect, use, modify, disclose, retain or dispose of personal health information are bound by certain obligations in PHIPA. These include not using personal health information except as necessary in the course of providing services, not disclosing personal health information, and not permitting employees or others acting on the supplier’s behalf to have access to personal health information unless they agree to be bound by these restrictions.

Further, if the supplier is a “health information network provider,” providing services to two or more health information custodians primarily to enable them to disclose personal health information to one another electronically, regardless of whether or not it is an agent, the “health information network provider” is subject to further obligations prescribed in regulation.

7 Available at: www.csa.ca/standards/privacy/code/
8 Available at: www.ipc.on.ca/images/Resources/up-gps.pdf
What Is Radio Frequency Identification (RFID)?

**RFID technology fundamentals**
RFID is a contactless technology that uses radio frequency signals to transmit and receive data wirelessly, from a distance, from RFID tags or transponders to RFID readers. RFID technology is generally used for automatic identification and to trigger processes that result in data collection or automation of manual processes.

Key advantages of RFID-based systems for health-care delivery include:

- Accurate identification without the need to touch (or even see) the RFID tag;
- Sensors can be incorporated into RFID tags to record temperature or identify positioning;
- Data stored inside RFID tags can be encrypted, modified and rewritten on demand;
- Tags are recyclable and can be made difficult to counterfeit;
- Special devices are required to read RFID tags, increasing privacy in some cases (e.g., in comparison to human-readable information).

The most common application types, grouped according to the purpose of identification, are presented below:

<table>
<thead>
<tr>
<th>Purpose of Identification</th>
<th>Application Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determine the presence of, and identify, an item</td>
<td>Asset management, safety</td>
</tr>
<tr>
<td>Determine the location of an item</td>
<td>Tracking, emergency response</td>
</tr>
<tr>
<td>Determine the source of an item</td>
<td>Authenticity verification</td>
</tr>
<tr>
<td>Ensure affiliated items are not separated</td>
<td>Matching</td>
</tr>
<tr>
<td>Correlate information with the item for decision-making</td>
<td>Process control, patient safety</td>
</tr>
<tr>
<td>Authenticate a person holding a tagged item</td>
<td>Access control, ID verification</td>
</tr>
</tbody>
</table>

Many RFID applications will often span multiple purposes.

An RFID system is typically composed of:

1. RFID tags, which can be Passive, Active or Semi-Active, typically containing a unique identifying data string and potentially additional data;
2. RFID readers and writers, which can be wireless, handheld or fixed reader/antenna devices;
3. An infrastructure, including middleware, that permits RFID readers and writers to process data to and from the RFID tags, manage communications, access control and security, connect to back-office applications, and take actions on the basis of that data.
It is important to note that the RFID tag and reader are only the up-front, visible part of an RFID system, which often connects through a wired or wireless network to a back-office application and one or more databases or hospital information systems.

There are some important types and varieties of RFID tags and associated RFID information technologies and systems. These are outlined briefly below.

1. **Passive vs. Active RFID tags**

   RFID tags can be Passive (non-battery powered), Active (battery-powered), or Battery-Assisted Passive (dual mode). Passive tags, which are by far the most common, are the simplest and least expensive to manufacture and use. They contain a chip and antenna on a substrate, typically attached to a label or bracelet, are typically classified within Low-Frequency, High-Frequency or Ultra-High Frequency groupings, and comply with standards such as ISO or Electronic Product Code (EPC). To transmit their data payload, passive tags use radio energy supplied by RFID interrogators or readers. Passive tags typically contain small data payloads, can be read-only or read-write, and must be physically close to the reader to communicate effectively (Hi-Frequency tag read-ranges can vary from 3 to 30 inches, Ultra-High-Frequency tags can be read up to 15 to 20 feet from the reader-antenna). The new generation of Battery-Assisted Passive tags can contain larger amounts of data, and transmit over longer distances.

   Active RFID tags, or transponders, contain a battery and can be configured to transmit their information at given time intervals or react to an awakening signal or event. The tag’s battery life typically ranges from one year to over five years, depending on the frequency that they transmit data. These tags are much more expensive than passive tags, but provide additional functionality. The tags can be read at longer...
distances (e.g., 100 to 500 feet), can hold larger amounts of data and can contain integrated sensors (e.g., temperature, motion, tamper-detection, etc.). Some active tags can provide two-way communications using customizable buttons, LED lights, or buzzers integrated into the tag, similar to a pager. This technology is typically used in high-value asset management solutions or real-time medical equipment tracking solutions, including detection of presence, zone coverage or real-time location services (RTLS). RTLS systems function in a manner similar to GPS location systems, measuring the signal strength from the tag received by three or more readers and graphically displaying the current or historical location of the tag on a map. Some RTLS systems use proprietary antennas and readers and others can leverage an existing Wi-Fi infrastructure to communicate with the tags. The systems can be configured to provide customized monitoring and alerting of events, such as battery power status, a tag entering a restricted area, a tag falling to the floor, or a tag being removed from an object without authorization.

All of the described types of tags have important implications for privacy and security.

2. Referential vs. non-referential RFID systems
The term “referential” is used for RFID systems using tags that typically contain a unique “key” or semi-random data string, which allows retrieval of relevant information from an application or database. Referential RFID systems are the dominant type in use today. As suggested by Figure 1 above, the data on the tags serves as a pointer or “reference” to a centralized storage and processing systems located elsewhere on the network. The information stored on the tag allows retrieval of information from the database, file, or document contained in the back-office system, or logic embedded inside a local or remote information system or process. For example, an RFID-enabled proximity card can contain a serial number that, when waved near an antenna connected to a reader, triggers that reader to collect the data and send it to a computer or server where the data is compared against stored values. If there is a positive match, an action is then performed, such as unlocking the door to an office or opening a patient’s medical record. If the network is down, the system may not function as desired, as the information contained in the tag may not be sufficient to trigger the desired action.

By contrast, “non-referential” RFID systems are able to store all or some of the data needed for systems operation in the tag’s memory, and may contain logic running on mobile devices or the tag itself. This functionality allows decisions to be made based on the information stored in the tag, without any need for linked networks and back-end databases to function, which can prove useful if the network is down, or the data can not be accessed online. Non-referential systems contain functionality to synchronize the information between the tag and a back-office database or application and encryption is typically used to protect against unauthorized access to the data.

Both types of RFID systems have implications for personal information and privacy.
3. Closed vs. Open Loop applications

A closed-loop RFID application – the most common type – is any RFID system that is deployed entirely within a single organization, rather than across several organizations. Closed-loop RFID information systems may involve the use of either standards-based or proprietary tags, encoding formats, transmission protocols, and processing middleware.

An open-loop RFID application, by contrast, is intended to function across organizational boundaries, requiring adoption of common standards and information-sharing protocols. RFID deployments for supply-chain management, in which an item is tracked across various organizations in a range of locations, are a classic example of open-loop RFID application.

Just as the authenticity of the RFID-enabled proximity card is verified against a back-end database, the authenticity of a pharmaceutical product may be verified to ensure that the product is not counterfeit. A record of access can be kept for billing purposes or to record the time that someone entered a particular building or room. The travels of an RFID-tagged item can be monitored and tracked across time and distance through periodic reads of the tag and correlation of its unique identification in a database. This is what occurs when RFID-tagged supplies and inventory are shipped from a production facility to a distributor to a retailer, providing visibility and accountability throughout the entire supply chain.

Sample RFID System

RFID Technology vs. Bar Codes

Bar code systems are commonly used in health-care settings, but are known to have technical limitations such as inaccessibility when a patient covers the wrist band with his or her body or the bar code is curved around a wrist band. In such
cases, manual entry of the patient ID is required, or the patient must be awaken or touched to facilitate reading of the bar code, potentially increasing the risk of nosocomial infections. Bar codes also have limited storage space for information and can wear out after protracted use. They do not facilitate modification and updating of information (unless the bar code is reprinted). These limitations consume resources that could otherwise be spent on other tasks, increase the risk of human error, and increase operating costs.

Generally speaking, RFID represents a next-generation improvement over traditional bar codes. Some differences between the two technologies are identified below.

<table>
<thead>
<tr>
<th>Bar Coding</th>
<th>RFID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requires line of sight</td>
<td>Line of sight not required</td>
</tr>
<tr>
<td>Scan one item at a time</td>
<td>Multiple items at a time</td>
</tr>
<tr>
<td>Inexpensive</td>
<td>More expensive</td>
</tr>
<tr>
<td>Widely used</td>
<td>Emerging application in health care</td>
</tr>
<tr>
<td>Standards-based</td>
<td>Standards developing</td>
</tr>
<tr>
<td>Read only</td>
<td>Digital, read-write capable</td>
</tr>
<tr>
<td>Depends on external data store</td>
<td>Can store data or trigger access to external data</td>
</tr>
<tr>
<td>Provides licence plate information only</td>
<td>Can store relevant data (serial #, loc., status, etc.)</td>
</tr>
</tbody>
</table>

**RFID and Privacy**

**RFID implementation considerations**

There are five general implementation issues associated with deploying RFID technology:

1. **Cost** – The cost of the technology (tags, readers, middleware, consulting, operational process design, troubleshooting, training, etc.) will impact return on investment (ROI) and value.

2. **Integration with hospital information or other back-office systems** – Legacy information systems may need to be modified or re-engineered to accommodate the RFID system, technology, and information.

3. **Reliability** – Depending on the operating environment, the intended purposes, the technology contemplated, and the deployment method being considered, RFID technologies may not deliver sufficient accuracy or performance results to be suitable for mission-critical applications and uses.
Security – RFID tags are susceptible to many of the same data security concerns associated with any wireless device. Passive tags in particular are considered to be “promiscuous” – automatically yielding their data to any device that queries the tag, raising concerns about skimming, interception, interference, hacking, cloning, and fraud, with potentially profound implications for privacy. While a variety of security defences exist, such as shielding, tag encryption, reader authentication, role-based access control, and the addition of passwords, these solutions can raise complexity and costs.

Privacy – If RFID tags contain personal information, which could include health information, or data linked to personally identifiable individuals, without the proper security or integrity mechanisms in place, privacy interests become engaged. Personal health information is among the most sensitive types of information. As such, it requires stronger justifications for its collection, use and disclosure, rigorous protections against theft, loss and unauthorized use and disclosure, strong security around retention, transfer, and disposal, and stronger, more accountable governance mechanisms.

Privacy-relevant properties of RFID systems
There are certain fundamental properties of all RFID information systems that are particularly relevant to privacy, regardless of the specific technology, application type, or deployment scenario.

1 Health-care providers must realize that RFID systems are a key part of an overall information system. Consequently, a holistic systems approach to privacy is warranted, rather than a strict focus on the interaction between tag and reader.

2 RFID tags contain unique identifiers, indicating not only the presence of an object, like an anti-theft tag, or a class of objects, like a product bar code, but also an individualized serial number. The ability to uniquely identify individual items has privacy implications when those items can through inference automatically be associated with people.

3 RFID tag data can be read (and sometimes written) at a distance, without “line-of-sight” and through many camouflaging materials, potentially without the knowledge or consent of the individual who may be carrying the tag. This has potent implications for informed consent.

4 RFID information systems can also capture time and location data, upon which item histories and profiles can be constructed, making accountability for data use critical. When such systems are applied to people, it may be viewed as surveillance (or worse, depending on what is done with the data).

9 For a discussion about various forms of wireless technologies and the privacy and security considerations in their use, see IPC Fact Sheet #14 – Wireless Communication Technologies: Safeguarding Privacy & Security (August 2007), available at: www.ipc.on.ca/images/Resources/up-1fact_14_e.pdf
To first understand privacy and security risks, and then to mitigate these risks, we must always follow the (personal) data as it flows throughout the entire information system: what data is collected, how and for what purposes, where it is stored, how it is used, with whom it is shared or potentially disclosed, under what conditions, and so forth. This is referred to as the information life-cycle, and the disposition and governance of personal health information throughout its life-cycle lies at the heart of most information privacy concerns in the health care environment.

RFID systems are, fundamentally, information systems put in place by organizations to automatically capture, transmit and process identifiable information. Informational privacy involves the right of individuals to exercise control over the collection, use, retention and disclosure of personally identifiable information by others. There are inherent tensions between the, at times, competing interests of organizations and individuals over the disposition of the information, especially over the undisclosed or unauthorized revelation of facts about individuals and the negative effects they may experience as a consequence.

As was described in a recent European study on the many uses of RFID technology, RFID information technologies can exacerbate a power imbalance between the individual and the collecting organization.10

**General approach and framework to building privacy in early**

Building privacy into information systems and technologies, whether RFID-enabled or not, begins at the top of the organizational decision ladder, and at the early stages of project design and implementation. A comprehensive, multidisciplinary approach is required. The steps outlined here provide a high-level approach and general framework for building privacy into information technologies and systems.

As a framework, it is useful for general orientation and planning purposes, and may be used as a starting point for deeper analyses, according to the specific objectives, operational characteristics, and other parameters of the RFID proposal or project in question.

1 Clearly define, document and limit purposes for collecting and using personal data, in order to minimize the potential for privacy invasion. The purposes identified should meet the tests of necessity, effectiveness, proportionality, and no less-invasive alternative.

2 Develop a comprehensive and realistic project management plan, with the pivotal involvement of a knowledgeable privacy officer, with sufficient authority and resources.

---

3. Identify all information security and privacy risks throughout the data life-cycle, including risks from inside the organization as well as external sources.

4. Conduct a comprehensive Privacy Impact Assessment (PIA) of the entire system at the conceptual, logical and physical stages of its development, with a clear plan and timetable for addressing identified risks.

5. Build privacy and security in at the outset. This means incorporating the principles of fair information practices into the design and operation of an RFID information system, and the policies that govern its operation.\(^{11}\)

6. Implement appropriate operational and systematic controls that can be measured and verified, ideally by independent entities, if necessary.

7. Review the operation and effectiveness of the RFID system, as well as related networking, data storage, wireless transmission, and data backup systems on a regular basis.

RFID systems may need to be highly customized to support the business processes they automate, and will depend on the types of back-office systems, medical information system, scheduling or similar support systems they must interface with. In many cases, a “one-size-fits-all” approach will not work across all health-care implementations. Good privacy and security practices, integrated with strong project management skills, can help health-care providers manage RFID risks to an acceptable level.

The section that follows goes into more detail on the privacy considerations specific to the RFID health-care application.

**RFID Applications in the Health Sector**

Health-care providers around the world have been using or testing RFID technology in a variety of contexts for several years. For example, RFID technology has successfully been used to tag pharmaceutical products to reduce the risk of counterfeit medications use in the United Kingdom.

RFID is also proving to be very useful in identifying patients, increasing safety and reducing incidents of mistaken identity during critical surgery. It is being successfully used to locate patients needing extra care, such as the elderly, or patients suffering from Alzheimer’s or memory loss.

Medical equipment is being more rapidly located and tracked within health-care facilities, leading to more effective use of resources. Waste management has been improved through the use of RFID.

---

From a privacy point of view, the single most relevant consideration is whether and to what extent the RFID-related data collected or generated from the tags may be characterized as personally identifiable (health) information. To the extent that it is (or could be) personally identifiable data, then legal and regulatory privacy requirements are invoked.

For this reason, we have organized some of the known RFID technology deployments into three broad categories of increasing privacy relevance and concern:

1. Tagging things;
2. Tagging things linked to people; and
3. Tagging people.

**Tagging things**

RFID technologies have proven to be ideal for identifying and locating things because they increase the reading accuracy and visibility of tagged items far beyond bar codes and other labels. The results can include greater efficiency for automating inventory processes, finding misplaced items, and generally keeping better track of things as they move through their life-cycles.

Automatic identification remains the basis of all RFID information systems, but specific applications may be variously described as asset management, tracking, authenticity verification, matching, and process or access control, depending on the context and circumstances. Application types are not mutually exclusive: an implementation or deployment can combine elements of several application types. For example, RFID-based information systems that both identify and locate tagged items combine asset management with tracking (real-time or otherwise).

All of these application types are currently being used by health-care providers, many of which are large institutions with complex asset management and logistical requirements.

Sample RFID health-care deployment scenarios that involve the tagging of things include:

- Bulk pharmaceuticals;
- Inventory and assets (e.g., trolleys, wheelchairs, medical supplies);
- Medical equipment and instruments (e.g., infusion pumps, wheelchairs);
- Electronic IT devices (e.g., computers, printers, PDAs);
- Surgical parts (e.g., prosthetics, sponges);
- Books, documents, dossiers and files;
- Waste and bio-hazards management.
One of the key reasons for introducing RFID-based automatic identification technologies and systems is often to improve operational efficiency. The integration of RFID technology with business intelligence and analytics systems has proven the benefit of leveraging this technology for business process improvement.

RFID tagging and tracking of items has also been shown to save valuable staff time and costs associated with manual data collection and input (especially when it is routine and repetitive), and also with physical searches for misplaced or lost items. Further, RFID-tagged assets and items can help reduce human errors and mistakes, as well as improve auditability and accountability, resulting in better quality health-care services.

Efficiency gains may also be realized from more accurate and up-to-date inventory accounting, and from reduced “shrinkage” of valuable assets.

Many pharmaceutical RFID tracking and tracing initiatives are underway in the U.S., E.U., and Asia. Pharmaceutical “drug e-Pedigrees” have become the subject of considerable attention by the health-care and RFID industries, as well as by government health regulatory and licensing agencies across North America.

A drug pedigree is a statement of origin that identifies each prior sale, purchase or trade of a drug product, including the date of these transactions and the name and addresses of all parties to them.

The U.S. Food and Drug Administration (FDA) e-Pedigree requirements were outlined in a 1988 set of FDA regulations enacted following the passage of the Prescription Drug Marketing Act (PDMA) of 1987, created to address problems of drug counterfeiting in the pharmaceutical supply chain. Pharmaceuticals can travel through many different points in the distribution chain from the factory to a pharmacy or hospital, creating a significant counterfeit drugs issue. To address these issues and ascertain proper “chain of custody,” the FDA has been investigating the use of RFID technology to increase supply chain security. At the time, the FDA anticipated that the e-Pedigree would be achievable by 2007.

The broad intent is to provide a documented chain of custody for high-value pharmaceuticals, from the production plant through to the dispensary, as well as the return and disposition of pharmaceutical items. In addition to automating the identification, documentation and pharmaceutical supply-chain management processes, drug pedigrees are also expected to help minimize incidence of counterfeiting and diversion, and to facilitate recalls.

Drug pedigree requirements can be fulfilled through traditional paper methods, but RFID technologies, combined with networked databases, offer a more automated, secure, and trusted way to establish such a pedigree.
Privacy Considerations

Generally speaking, the business of identifying and tracking inventory and objects does not involve collection, use or retention of personally-identifiable information. The uniquely identifying data stored on the RFID tags, which are read by interrogators, transmitted across networks, processed by middleware, stored in logs, shared with third parties, and acted upon in the context of relevant business processes, refers exclusively to “things” in a manner analogous to a product serial number. Accordingly, if there is no personally-identifiable health information, then privacy does not come into play.

In February 2004, the U.S. Food and Drug Administration recognized the potential of RFID information technologies to combat counterfeit pharmaceuticals and to provide more effective fulfillment of U.S.-mandated drug pedigree requirements.\(^\text{12}\) In November 2004, the FDA issued a report recommending that drug makers use RFID to track bottles of the most commonly counterfeited drugs, with eventual extension to more drugs over time.\(^\text{13}\) The FDA also published a guidance policy around the use of RFID in the pharmaceutical industry, which states, \textit{inter alia} that:

- RFID tags are attached only to immediate containers, secondary packaging, shipping containers and/or pallets of drugs that are being placed into commerce;
- Drugs involved will be limited to prescription or over-the-counter finished products;
- RFID will be used only for inventory control, tracking and tracing of products, verification of shipment and receipt of such products, or finished product authentication;
- The tags will not contain or transmit information for the health-care practitioner or the consumer;
- The tags will not contain or transmit advertisements or information about product indications or off-label product uses.

The scope of the FDA’s guidance makes clear that personally-identifiable information is not involved in the pharmaceutical supply chain management, and hence, privacy issues, do not come into play.

Examples of RFID Uses

The following examples provide a glimpse into the broad range of uses for which RFID technologies may be deployed by tagging things:


High Value Mobile Equipment: The ambulatory care centre of a large Boston-area hospital is using RFID to track and maintain more than 1,500 units of high-value mobile medical equipment, including wheelchairs, gurneys, portable oxygen tanks, intravenous (IV) pumps and defibrillators. The prices of these assets range from a few hundred dollars apiece to several thousand, and many of them, such as IV pumps and wheelchairs, need to be maintained on a regular schedule.

Cardiology Devices: A Detroit Medical Centre is installing an RFID deployment to track the institution’s growing number of medical devices. The RFID solution will be deployed for the cardiology group. Fourteen RFID-enabled cabinets will be installed to store implantable stent devices. The goal is to streamline and automate the management of these devices. Time lost to the current manual processes will be recaptured, and the documentation of device usage and expiration will be made more accurate.

Infusion Pumps: A large health-care system in Georgia is deploying an RFID asset-tracking system to improve management and utilization of thousands of tagged infusion pumps and other high-value equipment.

Location Tracking: According to one RFID vendor, a large, multi-hospital health-care provider is installing a real-time location system that uses hybrid Radio Frequency tags, combined with infrared (IR), to pinpoint the exact room in which an asset is located. The health-care provider has performed a beta test of the RF-IR system in which each hospital room is fitted with a Room Locator, an IR transmitter designed to send a location-identifying code.

Surgical Sponges: An independent organization, “No Thing Left Behind,” is halfway through clinical trials testing RFID-enabled sponges, interrogators and companion software, in surgical cases in five different medical centres across the United States. The No Thing Left Behind project’s overall objective is to help hospitals, surgeons, perioperative care nurses, and patients work together to ensure that surgical tools used in an operation are never left inside a patient. Recent studies have estimated that cases of surgical objects left in patients occur in between one out of every 100 to one out of every 5,000 surgical procedures. Other studies have shown that two-thirds of all retained foreign bodies are surgical sponges.

Medical Waste: Hospitals deal with hazardous waste on a daily basis, so a comprehensive system is necessary to manage and dispose of it safely and efficiently. Usually outsourced to service providers, waste management is a matter of concern to many hospitals. They are unable to control the vendor’s work processes and can’t be certain if wastes will be handled in compliance with the work contract or local legislation. One RFID solution for waste management provides proof-of-delivery and receipt, as well as location tracking and activity records to ensure the integrity. Sealed waste containers are tagged with locked RFID bands that keep track of the container movements, ensuring that potentially hazardous waste is not
compromised en route to the waste management plant from the hospital. At the destination plant, the RFID bands automatically transmit information such as the arrival time, quantity and weight of waste back to the hospital for accountability.

**Robotic Hospital Helpers:** A Pittsburgh company has developed a hospital robot to perform such mundane but vital tasks as retrieving and delivering drugs and test specimens. Now, six of the more than 34 hospitals already using the robots are testing an RFID-enabled version, which carries an RFID interrogator used to locate RFID-tagged assets as it moves around a hospital. The robot finds its way around a hospital through the use of a facility map saved to its memory.

**Guidance**

Generally speaking, where there is no personally identifiable information collected or used by an RFID-based information system, and little likelihood or risk of RFID-generated data becoming personally identifiable information, then there are no privacy issues and, in Ontario, the provisions of PHIPA do not come into play.

In a similar manner, to the extent that pharmaceutical tagging and e-pedigree programs remain strictly a (bulk) supply-chain management issue, ending at the dispensary, the privacy implications are minimal, while the benefits may be considerable. The application of clear rules and guidance by regulatory agencies, such as by the FDA, will help to provide additional assurance and confidence that privacy interests are not engaged.

**Tagging things linked to people**

The next class of RFID technology uses involve RFID tagging of items that are (or may be) linked to identifiable individuals and to personal information, usually on a more prolonged basis (ranging from one week in the case of tagged garments, to several years or longer in the case of patient dossiers).

Some RFID deployment scenarios that involve tagging things linked to people include:

- Medical equipment being used by patients, visitors or staff;
- Readers, tablets, mobile and other IT devices assigned to staff;
- Access cards assigned to staff or visitors;
- Smart cabinets;
- Devices, garments, or spaces (rooms) assigned to patients;
- Blood samples and other patient specimens;
- Patient files and dossiers; and
- Individual prescription vials.

For more FDA info and guidance, see [www.fda.gov/oc/initiatives/counterfeit/](http://www.fda.gov/oc/initiatives/counterfeit/)
In each usage scenario, the main purpose of the tagging is to identify and track objects, as before, but the relative permanence of the tag, the nature and amount of the data collected, and the strength of the data’s linkage to identifiable individuals may invoke privacy issues and concerns.

Privacy Considerations
Increasingly, RFID tags are being attached to items that are, or may be, linked to individuals. Privacy interests become progressively engaged with the strength and ease of this linkage, along with the sensitivity of the linked data. The same basic properties that make RFID information technologies and systems so useful for inventory control and supply management purposes can impact individual privacy when that tracking and control extends to individuals, especially when informed consent is lacking.

There are asset identification, tracking and management scenarios that could involve a link with personally identifiable information. For example: all touch-points or interactions with tagged items (and the data generated) by staff might be logged for audit and accountability purposes, engaging employee privacy interests. Tagged assets could also be temporarily assigned to individuals (beds, rooms, equipment) and, if they are mobile items, can become a proxy for tracking people through inference. Even if the data on an RFID tag is encrypted or otherwise unintelligible, the tag can still be used as a basis for tracking and its history correlated with personally identifiable information from another system. This could happen, for example, when use of an RFID-enabled visitor access card is correlated with a video capture of the bearer, at access points or other chokepoints.

Some RFID tags are re-writable and re-usable. If data about an individual, such as a patient identifier or drug prescription, is written locally to the tag, then it is possible it may be read and used in an unauthorized manner if it is not properly secured or destroyed.

If the RFID-tagged item travels with the individual, then extensive tracking and monitoring of the item is tantamount to tracking and surveillance of that individual. In the case of access cards, the threats and risks extend to hacking and cloning of the embedded RFID tags, allowing unauthorized individuals to effectively access secure spaces and to commit identity theft.

Unauthorized identification, tracking, surveillance, and profiling of individuals are very serious privacy issues. In addition, security issues related to RFID tags, including skimming, eavesdropping, interception, interference, tampering, cloning and misuse, can also impact individual privacy (as well as the operations of healthcare providers).
As noted earlier (see “referential vs. non-referential systems”), RFID tags do not always contain personally identifiable information, such as a person’s name. In most cases, they encode some semi-random unique alphanumeric string that can serve as a pointer, or index key, to a person’s linked identifiable information, such as a medical or transaction record stored in a networked database (perhaps even transmitted offsite and controlled by third parties). RFID readers – often mobile – read tag data and use it to trigger an action, such as to display and record the tag contents, or to “look up” and retrieve (and use) data corresponding to the tag ID.

Readers themselves, or any RFID-enabled portable computing and communications device, may be assigned to health-care personnel to help them collect and transmit data stored on tags elsewhere. Usually this is intended to help staff accomplish their tasks faster and more efficiently, but the data collected can then be correlated with the personnel ID or role, and used to establish audit trails and to enhance accountability.

Generic (i.e., blank) RFID-embedded access cards may not serve as identity cards, yet their assignment to staff and permissible uses are controlled centrally. Typically, there is some linkage with identified individuals (i.e., the bearer), and all uses and attempted uses of the cards are routinely collected and retained in logs. This allows for the possibility of detailed profiles to be constructed.

Tagging patient specimens and other waste for proper handling or disposal may actually enhance privacy if the alternative involves labelling the item with human-readable personally-identifiable information or bar codes. As usual, much depends upon the strength of the linkage to the patient and the ease with which parties may make that connection (e.g., database access). In general, however, any tagged file or item that must be linkable to an individual, yet be passed around to multiple parties in a privacy-preserving manner (e.g., admission slip, test results, survey results/feedback, files, etc.), could potentially benefit from the deployment of RFID technology.

While the concern here is with the privacy and security issues related to RFID technologies, there will be very justifiable and defensible health-care-related reasons for deploying such technologies even where there are informational privacy implications. In these circumstances, it is important that the benefits be demonstrable, the privacy risks identified and properly mitigated, and the entire system developed and deployed in a transparent, and responsible manner.

Examples of RFID Uses
The following deployment examples provide a glimpse into the broad range of uses for which RFID technologies for tagging things linked to people may be deployed:
Hand-washing compliance: To reduce the spread of infections, a new automated hand-sanitizing system uses RFID to monitor how well health-care workers wash their hands. The wash cycle automatically starts when the caregiver’s hands are inserted into the machine’s cylindrical openings. Health-care-associated infections affect nearly 2 million individuals annually in the U.S., and are responsible for approximately 80,000 deaths each year, according to a guide published by the Centers for Disease Control and Prevention (CDC), in collaboration with the Infectious Disease Society of America (IDSA) and the Society of Healthcare Epidemiology of America (SHEA). The transmission of health-care-related pathogens most often occurs via the contaminated hands of health-care workers. When washing hands, a caregiver wearing an RFID badge is identified by the machine’s RFID interrogator. The device records the date and time, as well as the beginning and end of the wash cycle, then communicates that information to the database. If a caregiver removes the hands before the 10-second cycle finishes, the interrogator transmits this information to the back-end database. Hospital administrators can then run departmental statistics and other compliance reports to determine which caregivers have completed the washing cycles.

Smart Cabinets: Texas University Medical Center researchers are using RFID to manage the supply of chemicals and other materials used in biology research. The Center has installed two storage cabinets fitted with RFID interrogators. Items stored inside the cabinets are fitted with RFID tags. Every authorized researcher at the university has been issued a credit card-sized RFID key card carrying a unique six-digit ID number that is used to release the lock. The interrogator reads the key card’s ID number and the item tags in the cabinet before and after it has been opened, enabling the software application to calculate what has been removed, and to update the online inventory data. This information is accessible via the Web by university administrators, researchers and suppliers, and generates e-mail messages to the school’s accounts payable department and to the person who removed the items. Besides recording each transaction, the system helps suppliers know immediately what supplies have been used, what needs to be paid for and what needs replacing.

Specimens: A well-known medical practice with diagnosis and treatment facilities scattered across the U.S. piloted an RFID system to allow medical practitioners to better manage specimens of patient tissue. Deployed at endoscopy facilities, the tissue samples are tagged and tracked from the moment they are collected until they are delivered to the pathology laboratory for analysis, a series of steps characterized as “crucial.” The pilot lasted five months, and the demonstrable benefits included accurate data communication and verification, as well as improved efficiencies in specimen management. The plan now is to rapidly phase in an expansion of the pilot.
Blood bags: In Malaysia, the government and three medical institutions are testing an RFID system for tracking blood bags, with the ultimate goal of eventually equipping more than 300 other government and private hospitals and clinics. The system combines blood bag tagging with smart cabinets to enable automated, efficient track-and-trace visibility. Eventually the system could manage Malaysia’s entire blood bank, which includes 500,000 transfusions annually. The expected benefits include improved blood bag identification, inventorying, and logistics. Cross-matching, in which a recipient’s blood type is matched to available donated blood, will be streamlined. Internal blood management processes will be made more efficient. Blood stock will be better maintained. Errors, blood-type mismatches, and waiting times will be reduced. Data management and access overall will improve, including easy report generation for inventory, donation history, and donor/patient profiles. Registration and results screening during the blood donation processes will be simplified. Lastly, the system will enable analytics for the entire blood bank management process.

Medicine Dispensing: A Southeast Asian RFID systems provider has introduced RFID-enabled products designed to help health-care providers track pharmaceuticals and monitor drug administration, to make sure that correct doses are given. The company’s intelligent medicine-dispensing system combines RFID tags and readers, workflow software, electronic medical records (EMRs), and a central database in an integrated solution. This enables nurses and doctors to view patient records, update them in real-time, and double-check prescription dosages at the moment they administer them. The system can also automatically send prescriptions to pharmacists.

Patient Files: An acute-care and teaching hospital in New Jersey is implementing an RFID-enabled patient record management solution. Seeking both increased efficiency and compliance with Health Insurance Portability and Accountability Act (HIPAA) (which places heightened importance on patient information management), the hospital has targeted its Sleep Centres, which provide comprehensive evaluation and treatment for patients experiencing sleep-related problems. The centres manage 5,000 patient files. Each file is tagged with an RFID tag, allowing it to be tracked from the moment it is created for a new patient until the file is retained in storage. RFID readers are positioned in key locations around the centre to enable automatic tracking and encoding of the tags as they are moved from one place to another. Reads and writes to the tags are dynamically updated in the central database, ensuring real-time, accurate location data. The centres also have a series of handheld readers for routine inventory and locating misplaced files.

Handheld Devices to Verify Medications: The St. Clair Hospital in Pittsburgh developed and implemented an RFID-based system to help protect patients from medication errors and reduce health-care costs. Using bar code and RFID technology and a wireless network combined with HP iPAQ Pocket PCs, the VeriScan medication administration verification system confirms that a nurse has the correct patient,
medication, time, dose and route each time a medication is administered. The system has been in use for two years and is preventing more than 5,000 medication errors yearly, according to the hospital’s chief operating officer. “With close to 1.3 million doses dispensed each year from St. Clair Hospital’s pharmacy, we have plenty of opportunities for medication errors.” The RFID system helps the hospital nursing staff avoid most of those errors and the associated costs, with estimated costs savings of more than $500,000 annually. When it comes time to administer a medication, the nurse uses an HP iPAQ Pocket PC to scan bar codes on the medication package and RFID tags on the patient’s wristband. The VeriScan software compares the two sets of patient and medication data and alerts the nurse to any discrepancies. New orders, changes to orders and discontinued orders are available in real-time so that the nurse is aware of medication changes without delay. Not only does patient information pop up on the handheld display screen, but also a picture of the patient, which was taken when the patient was admitted. The device records the date and time the tags and bar codes are read, and then wirelessly sends all the data (bar codes, RFID tag numbers, and timestamp) to the database, where it is compared with the doctor’s latest orders. Voice commands on the handheld announce, “Patient identification confirmed,” or, in the case of discrepancies, “Access denied.” In addition, any new medication orders, order changes or cancellations are automatically downloaded so that nurses can learn about them immediately.

**Pharmaceutical tagging (item-level):** While most industry efforts are directed at realizing the benefits of tagging and tracing bulk pharmaceuticals in the supply chain, as discussed earlier, a smaller subset of initiatives is investigating the benefits of tagging item-level drugs, or even individual prescriptions, usually in more limited health-care provider contexts.

As noted in some of the case studies above, health-care providers are seeing merit in tagging and tracking specific drugs within their own care environments, principally to reduce patient medication errors and also to maintain accurate inventory records. Using RFID technology, specific drugs may become associated with patients and staff in the course of their use, helping to provide an accountable and auditable record.

More ambitious RFID pilot projects involve integrating the technology into medication packaging for monitoring, patient diary and reminding purposes. In these cases, RFID technologies serve as an automated mechanism for ensuring that patients are taking the correct drugs, in the right dose, at the right times, perhaps for clinical testing and recording purposes. The informed prior consent of the patient is critical in such scenarios.

Less clear is the extent to which prescription vials provided directly to individuals by pharmacies are currently being RFID-tagged (for example, to help track and speed up refills). This use case scenario presents the strongest privacy issues, i.e., the
possibility that individuals may carry on their persons RFID tags containing sensitive prescription information that could be scanned and read by unauthorized parties.

Patients have a legitimate right to know how easy it would be for unauthorized parties to scan and read the contents of personal prescription vials carried in a purse or pocket, and to be given a non-RFID alternative choice. Personal health information that may be inferred from the drugs a person takes is highly sensitive, and requires strict controls and assurances against unauthorized disclosure and collection. Efficiency and convenience should never automatically trump privacy interests!

Guidance
To the extent that personal information is involved and potentially at risk, we urge moving forward with caution, diligence, and a comprehensive information governance program. When assessing the extent of personally identifiable information involved and the degree of risk involved, the following important questions should be asked regarding the system design and information flows:

- Whether personal information is stored on the tags;
- Whether the tagged items are considered personal;
- The likelihood that the tag will be in the proximity of compatible unauthorized readers;
- The length of time records are retained in analytic or archival systems; and
- The effectiveness of RFID security controls, in particular:
  - The efficacy of tag memory access control and authentication mechanisms;
  - The ability of tags to be disabled after use; and
  - The ability of users to effectively shield tags to prevent unauthorized reading.

Prescription tagging: If and when RFID tags are affixed to individually prescribed vials, pharmacies and health-care providers will have to address a number of privacy questions and concerns:

- Objective of tagging vials – are they clearly defined? Combating pharmaceutical counterfeiting, fraud and diversion are less compelling reasons at the individual prescription level.

- An account of any (new) information vulnerabilities and threats, and appropriate countermeasures to mitigate them. How easy is it for others to read and understand the contents of the tagged vials? Can these vulnerabilities be addressed through information security measures, such as encryption or shielding, and through better patient education?

- Do your privacy policies and procedures extend to the handling of RFID-tagged vials? Do they cover any potential use or misuses of the tag and its data?
Tagging **people**
The third and final class of RFID uses involves the intentional tagging and identification of individuals, rather than the devices, tokens or other assets they may be carrying or associated with. The distinction can be subtle since, technically speaking, it is always the tag that is identified in any RFID systems. However, when we talk about tagging people, we are focusing on the primary purpose of the RFID deployment in question, as well as the relative strength and permanence of the linkage of the tag to the individual and his or her personal information.

For example, we would exclude from this category a generic or reprogrammable RFID-enabled access card that is temporarily signed out for use by an employee, contractor or visitor. The primary purpose of the card is to authorize physical access to certain facilities or spaces, rather than identifying the bearer. The card assignment may be temporary in nature, and the card contains no specific personally identifiable information embedded or on its face. Any linkage of the card ID to the individual is retained only in a central register rather than for operational use. Someone else may use the access card at a later date.

Examples of RFID used (or intended to be used) to identify and track individuals in health care contexts include:

- Health-care employee identification cards;
- Patient health care identification cards;
- Ankle and wrist identification bracelets (e.g., for patients, babies, wandering or elderly patients); and
- Implantable RFID chips.

The assignment of temporary RFID-enabled bracelets or anklets to patients for the duration of their hospitalization and treatment, especially in large facilities, can help reduce the risk of patient misidentification, wandering or treatment error.

RFID-enabled bracelets are being effectively used by many hospitals and health-care facilities as alternatives to printed bar code identification to securely identify patients. Consent is typically provided or implicit, in the same manner as would be provided to allow identification through the use of a bar code or human readable tags.

The practice of assigning RFID-enabled bracelets to newborn babies, in order to prevent inadvertent mix-ups or abduction, is considered to be a reasonable, proportional and effective measure. One such maternity identification program also assigns a matching RFID to the mother, for added assurance, in order to confirm the match between mother and child.

In many cases, the use of RFID wristbands, surprisingly, offers better patient privacy due to the fact that confidential and often sensitive medical information can be securely stored in the RFID tag, or accessed automatically from a centralized system rather than printed in human-readable format on the band itself.
Other examples include tracking medical researchers who work with bio-hazardous and contagious materials, where records of all movements and interactions are imperative.

RFID-embedded ("contactless") identification cards are a special category of health-care RFID use. Here we must distinguish between employee identification (and access) cards (whether “smart” or not), and patient identification cards. Employee Identification cards are increasingly being equipped with RFID technologies in order to identify and authenticate the bearer and facilitate access to physical spaces and other (e.g., computer) resources, as well as for process control and audit purposes. Dual or multi-purpose employee identity cards can serve differing functions at different times, according to context. Such a multi-purpose card and the data it contains, if not properly controlled, invites over-identification for some functions, function creep, and unwanted employee profiling.

Patient identification cards are used by health-care facilities to facilitate patient admission, treatment, and record-keeping. Given that personal health information is highly sensitive, significant security and privacy concerns would need to be addressed. The value of the embedded RFID data, if cloned, could be especially high since it may be obtained by stealth and used to obtain free health care by anyone capable of cloning the card’s contents (or acquiring a cloned card). This could open the door to identity fraud and theft.

Perhaps the most controversial use of RFID for tracking people involves implanting small RFID chips inside human bodies, typically below the skin of the upper arm. Approved by the U.S. Food and Drug Administration in 2004, RFID implants are being trialled in a number of non-medical scenarios, including military, employment, financial and recreational. In the health-care realm, voluntary RFID implant programs exist for individuals wishing to allow automatic identification and retrieval of their medical records by virtue of a 16-digit number correlated to information stored on a secure database. New RFID-based implants can also act as biosensors and as micro electro-mechanical systems for monitoring health conditions.

Generally speaking, if an RFID patient identification program responds to a defined problem or issue in a limited, proportional and effective manner, and is deployed in a way that minimizes privacy and security risks, at least as effectively as any alternative solution, then in principle there should be few privacy concerns with the program.

**Privacy Considerations**

Few topics elicit such strong views among the privacy community, medical practitioners, ethicists, consumer and civil rights groups, technologists, and public policy and lawmakers than proposals for using any type of technology to automatically and remotely identify and track human beings without their consent.
The prospect of remote, automated identification and tracking of individuals goes straight to the heart of critical privacy fears and concerns about RFID technology. These fears include:

- Surreptitious identification of individuals by known and unknown parties, without their prior knowledge or consent;
- Systemic tracking and surveillance of individuals by known and unknown parties, without prior knowledge or consent;
- The construction of histories and profiles about individuals and their interactions, without the individual's prior knowledge or consent;
- Correlation of acquired data with contextual and other information obtained elsewhere;
- Unwanted or incorrect inferences about the individual derived from the data;
- Unauthorized revelation of personal and private facts and disclosure to others;
- The inherent imbalance of power and potential for undesirable social engineering, control and discrimination on the basis of RFID-generated data;
- Unauthorized access, theft, and loss of RFID-based personal data held by custodians;
- Unauthorized interception and access to protected information stores by unknown parties, due to poor information security practices;
- The cloning of RFID identification data and possibility of unauthorized access to physical and logical resources, and of identity theft;
- The negative consequences upon the individual of all the above activities;
- The inability of individuals to find out about the collection and misuse of their data, and to remedy any errors or abuses; and
- The lack of confidence and trust by individuals in the information management practices of organizations.

More than two dozen U.S. states have, in the past two years, introduced bills intended to specifically restrict or otherwise prescribe the use of RFID for human identification and tracking.

At least three states have enacted laws to ban mandatory RFID “chipping” of individuals. Highly contentious public proposals for large-scale RFID-enabled passports, travel documents, enhanced driver’s licences and other portable documents continue to be actively debated, with privacy concerns at the forefront.

It is interesting to note the complexity and contentiousness of the matter for civil society. Few of these proposals, however, deal with health-care scenarios. One major exception is the subcutaneous “chipping” of patients, such as for long-term care patients suffering from Alzheimer’s or dementia, who may be incapable of reliably identifying themselves for proper care and treatment, and are prone to wandering.
The practice of subcutaneous chipping has been approved by the U.S. Food and Drug Administration as safe, and at least one U.S. company offers a nationwide program for individuals to voluntarily become chipped in order to be identified faster by participating caregivers, especially if unconscious or otherwise unable to communicate. The chip contains a short alphanumeric string that, when queried against a secure database, allows rapid access to personally-stored health records.

The U.S. Council on Ethical and Judicial Affairs (CEJA), which develops policies for the American Medical Association, issued a report (2007) saying that implantable RFID devices may compromise people’s privacy and security because it is yet to be demonstrated that the information in the tags can be properly protected.

Complex legal and ethical questions are invoked by RFID (and other ICT) implants in the human body. Many of these questions were addressed by the European Group on Ethics (EGE) in Science and Technology to the European Commission. In its 2005 report, the EGE stressed that RFID (and other implants) in the human body can have repercussions for human dignity, and that their use for health-care requires informed consent, utmost transparency and strict limits in the case of patients unable to consent. Implants to gain control over the will of people should be banned, and the autonomy of the patient is the yardstick.

Apart from subcutaneous chipping of the hospitalized elderly, there may be other justifiable reasons and circumstances for using RFID technologies in a less-invasive and less-permanent manner, to identify staff and patients. At least one elderly-care treatment centre assigns the elderly an active tag on a lanyard, allowing staff to automatically monitor and track the location of patients as they move about the facilities, and to respond immediately in the event of an incident.

**Examples of RFID Uses**

**Patient ID system:** In January 2007, HP and Precision Dynamics Corporation (PDC) announced the deployment of a comprehensive RFID-based patient management system at the Chang-Gung Memorial Hospital (CGMH) in Taiwan. The system offers the medical facility numerous benefits and has already realized positive results in patient identification. Patients are given wristbands with embedded RFID chips that increase the accuracy of patient identification and decrease the risk of so-called “wrong-site” and “wrong-patient” surgery, in which the incorrect operation is performed on the correct patient, or the correct operation is performed on the incorrect patient. Under the new system, CGMH has realized 100% accurate patient identification in the operating room. The system also automates data gathering, which cuts down on previous human error resulting from oral communication and manual data entry. This automation also yields better compliance with standard operating procedures. Alerts are generated in real-time when the sequence of a prescribed process is going amiss. In addition to improved accuracy, the HP-PDC
system brings improved efficiency. Medical staff now spend 4.3 minutes less verifying patient data per incident. This figure multiplied across hundreds or even thousands of daily patients (CGMH is part of an 8,800-bed health-care system) can bring dramatic savings and, ultimately, better health care. Lastly, the RFID wristbands offer better patient privacy in that the confidential and often sensitive medical information is stored on the RFID chip rather than printed in plain view on a wristband.

**Wi-Fi Elderly Care:** An Australian provider of elderly care is using a Wi-Fi-based RFID system to enable residents to quickly and easily call for help when they need it. The medical alerting system notifies caregivers any time a resident wanders into a dangerous area or hasn’t moved for a long time, indicating that they may need help. Affixed to lanyards that can be worn around the neck, the tags measure approximately 2 by 1.5 inches and are a half-inch thick. They are water-resistant and feature large, easy-to-find call buttons that residents can press when they are in trouble or need assistance. Staff also wear the tags so they can easily issue an emergency alert. When a tag’s call button is pressed, the tag transmits its unique ID number to a nearby Wi-Fi access point, which passes that information on to each staff member’s mobile handheld device, as well as to flat-screen monitors installed throughout the complex. The system can identify the room in which a tag is located, and includes a set of configurable rules designed to trigger alerts when broken.

**Patient Monitoring:** A Belgian University Hospital may be the first to use RFID technology not just to track where patients are, but how they are. The hospital is using Wi-Fi RTLS tags integrated with medical monitoring equipment to remotely transmit patient health data and emergency alerts. Nurses carrying wireless phones can instantly access patient information from the monitoring equipment, including blood pressure, oxygen level, and even electrocardiogram images. In case of emergency, the RTLS tags can automatically issue an alert. The system is currently being deployed at a 1,100-bed hospital. The integrated system includes the hospital’s legacy Wi-Fi wireless network, Wi-Fi-enabled RTLS tags, wireless phones, a Wireless Location Appliance, various communication technologies, and monitoring equipment from a major medical systems manufacturer. The tags are placed on monitoring equipment assigned to cardiology patients, who are then free to take strolls, visit lounges, and move about the facility. The application will provide patient location data in addition to advanced medical telematics information.

**Protecting Newborns:** Each year in the U.S., there are 100 to 150 baby abductions, with more than 50% of those babies taken from health-care facilities. There are also over 20,000 mix-ups, with the majority caught before the parents even know. A Dallas hospital was the first hospital to implement the “Hugs and Kisses” RFID system, which uses active RFID tags to tag babies and mothers. A “Hugs” tag is attached to the baby’s foot. Mothers wear a “Kisses” wrist band. If they pick up the wrong baby, they hear an audible alarm, while picking up the correct baby results in
a confirmation. RFID reader installations mean that any attempted abduction is detected as the baby is moved, with the system linked to CCTV and security. The tags are disabled after a time lock when the fire alarm has been activated. Over 400 U.S. hospitals are currently using the RFID-based baby and mother monitoring system.

**Medical Implant:** Doctors at the University of Texas Southwestern Medical Center, working with engineers from the University of Texas, Arlington, have developed innovative RFID-based medical technology to detect gastroesophageal reflux disease, caused by stomach contents moving up the esophagus. The condition, commonly referred to as esophageal reflux or GERD, is estimated to affect as many as 19 million people. The new solution combines RFID with sensor technology to measure and transmit data from within a patient’s body. A dime-sized RFID chip is inserted into the esophagus, where it remains pinned until a physician removes it. Equipped with an electrical impulse sensor, the chip measures particular impulses that indicate the presence of acidic or non-acidic liquids in the esophagus. These collected measurements are transferred from the RFID chip to a wireless receptor hanging around the patient’s neck.

**Implants:** In September, VeriChip Corporation, a provider of RFID systems for health care and patient-related needs, announced that more than 90 Alzheimer’s patients and caregivers received the VeriMed™ RFID implantable microchip at the official launch of their Project with Alzheimer’s Community Care. VeriChip’s collaboration with Alzheimer’s Community Care consists of a voluntary, two-year, 200-patient trial to evaluate the effectiveness of the VeriMed™ Patient Identification System in managing the records of Alzheimer’s patients and their caregivers.

**Guidance**

Because RFID technology allows for the automatic identification of identifiable individuals, special vigilance is required when tagging people. The privacy and security risks associated with collecting, processing, and retaining personal information are the greatest here, and require the strictest, most rigorous and most transparent application of project management skills and risk mitigation measures.

Subcutaneous RFID chips appear to be the most extreme form of using RFID technology to identify humans with its inherent risks. The majority of deployments, however, involve the simple assigning of an RFID-embedded card or bracelet to an individual. When pursuing this type of identification purpose, the following important design parameters should be considered:

- Whether the RFID tags will directly encode personally identifiable information, or serve as pointers to PII stored elsewhere;
- Whether the tags and their data will be part of an “open-loop” system (i.e., involving multiple organizations and actors);
• Whether the data will be stored or controlled by outside third parties;
• Whether and to what extent the tags are vulnerable to tampering and cloning;
• Whether and to what extent the tag and its contents will be under the control of the individual;
• Whether the tags will be active or passive, read-only or re-writable;
• Whether the tag is temporary or otherwise removable from the individual (e.g., bracelets, anklets, lanyards, implants, ID or namecard or other token); and
• Whether the tag’s unique data, or tag itself, will be permanently destroyed once its use expires.

Professional and Ethical Considerations
Whenever considering, designing and implementing information systems that involve collecting, using, retaining and disclosing sensitive personal (health) information of patients, health-care providers are strongly advised to consult appropriate professional codes and other codes of ethics. When in doubt, always check with additional sources.

In Canada, many such policies, guidelines and codes for the ethical uses of health information have been developed and are readily available. Readers are encouraged to visit the following useful websites:

• Canadian Institute for Health Research (CIHR): Policies and Guidelines in Ethics at: www.cihr-irsc.gc.ca/e/29335.html

• Developing a quality criteria framework for patient decision aids: online international Delphi consensus process at: www.bmj.com/cgi/content/full/333/7565/417

• Ethics in Mental Health Research at: www.emhr.net/ethics.htm
Conclusions

In this paper, we have described RFID technology, provided examples of current uses, and discussed its suitability for the health-care sector. RFID offers many potential benefits in a wide variety of health-care contexts for improving the safety, efficiency and effectiveness of health-care delivery. However, if not implemented with due care, it can also impact privacy interests in profound and negative ways.

We have grouped together three different classes of RFID deployment and described, at a general level, some of the security and privacy issues that could arise. We have suggested the use of various privacy-enhancing methodologies, tools, and techniques intended to ensure that privacy safeguards are built into information systems from the very start, sufficient to mitigate known vulnerabilities, threats and risks. The resulting RFID systems should merit the confidence and trust of all users and stakeholders, as well as meeting legislative compliance requirements.

The first class of RFID use involves the tagging of “things” alone, with no linkage to personal identifiers and, accordingly, no privacy issues.

The second class involves the potential for data linkage to personal identifiers, raising the possibility that individuals could be identified and tracked. This calls for the introduction of strong privacy-protective measures to ensure that no unintended consequences arise.

The third class involves the use of RFID intended precisely for the purpose of identifying people, thus serving as personal identifiers. While strong privacy measures are clearly required here, the concern with unintended consequences in this category is arguably less than in the previous one, where data linkage with personal identifiers is ancillary to the primary purpose. Care must always be taken, however, regardless of the extent of the threat posed, for strong protection of privacy.

We must ensure that Fair Information Practices – the heart of privacy and data protection – are clearly understood and implemented. Doing so invariably paves the way to preserving our privacy.

The authors gratefully acknowledge the work of Fred Carter, Senior Policy & Technology Advisor, Office of the Information and Privacy Commissioner of Ontario, and the HP Canada Emerging Technologies Team in the preparation of this paper.
RFID Resources

RFID Technology Information Sources
- GS1 EPCglobal:
  - GS1: www.gs1.org
  - EPCglobal: www.epcglobalinc.org
  - Discover RFID: www.discoverrfid.org
- RFID Journal: www.rfidjournal.com
- RFID Update: www.rfidupdate.com

RFID & Health Care/Life Sciences
  www.rfidjournal.com/article/articleview/3777
- Informationsforum RFID, *RFID for the Healthcare Sector* (August 2007), at:
  www.info-rfid.de/downloads/RFID_-_-for_the_Healthcare_Sector.pdf

    www.ama-assn.org/ama1/pub/upload/mm/467/ceja5a07.doc

  - IDTech Ex, *RFID for Healthcare and Pharmaceuticals 2007-2017*, at:

RFID & Privacy
- Office of the Information and Privacy Commissioner (IPC) of Ontario (Ann Cavoukian, Ph.D.), www.ipc.on.ca
  - Overview of RFID Privacy-Related Issues (2006), Presentation by the Commissioner to EPCglobal Inc (July 2006), at:
    www.ipc.on.ca/images/Resources/up-2006_07_20_IPC_EPCglobal.pdf
RFID Use Guidance

- Privacy Guidelines for RFID Information Systems (RFID Privacy Guidelines) www.ipc.on.ca/images/Resources/up-1rfidgdlines.pdf
- Practical Tips for Implementing RFID Guidelines www.ipc.on.ca/images/Resources/up-rfidtips.pdf

- Electronic Privacy Information Center (EPIC), Privacy Implications of RFID Technology in Health Care Settings presentation to the U.S. Department of Health & Human Services (2005), at: www.epic.org/privacy/rfid/rfid_ncvhs1_05.ppt


• RFID Position Statement of Consumer Privacy and Civil Liberties Organizations, at: www.privacyrights.org/ar/RFIDposition.htm

• Halamka, Juels, Stubblefield, and Westhues, The Security Implications of VeriChip Cloning, at: www.jamia.org/cgi/content/abstract/M2143v1

**RFID & Security**


• RSA Laboratories, RFID Privacy & Security, at: www.rsa.com/rsalabs/node.asp?id=2115

• Demo: Cloning the Verichip, at: http://cq.cx/verichip.plRSA

• “Security Analysis of a Cryptographically-Enabled RFID Device” at: www.usenix.org/events/sec05/tech/bono/bono.pdf

Privacy-Enhancing Technology (PET) Award Press Release at: www.microsoft.com/emea/presscentre/pressreleases/20062007PETawardsTS.mspx
Adding an On/Off Device to Activate RFID Tags in Enhanced Driver’s Licences: Pioneering a Made-in-Ontario Transformative Technology That Delivers Both Privacy and Security
There are well-known privacy and security vulnerabilities associated with Radio Frequency Identification (RFID) technology. So when I learned that the inclusion of an RFID would be a non-negotiable feature of Ontario’s Enhanced Driver’s Licence (EDL), my first thought was, “How can we transform the RFID into a technology that performs its functionality and is protective of privacy?” The RFID technology chosen by the U.S. Government for the EDL will respond not only to the authorized readers at the Canada-U.S. border, but also to any number of commercially available RFID readers which may be used surreptitiously. Therefore, it is imperative that holders of an EDL be able to prevent the RFID from being read by unauthorized third parties and disengage the RFID when not required for border-crossing purposes.

Since the ’90s, I have been promoting the concept of “Privacy by Design,” a term I developed to capture the idea of embedding privacy into the design specifications of technology – making privacy the default. I have never believed that the relationship between privacy and security had to be characterized as a zero-sum game, meaning that the more you have of one interest (security), the less you can have of another (privacy). I favour a positive-sum paradigm wherein adding privacy measures to otherwise privacy-invasive systems need not weaken security or functionality, but rather may, in fact, enhance the overall level of protection. I strongly believe that, by extension, my concept of Privacy by Design can be applied to the use of RFID technology in the EDL.

In my October 2008 submission and testimony to the Ontario Legislature’s Standing Committee on General Government on Bill 85, I recommended that, “The Ministry must work with a selected vendor to pursue adding a privacy-enhancing on/off device for the RFID tag embedded in the card” (Recommendation 4). This is the privacy-enhancing solution I am promoting to safeguard the use of RFID technology in Ontario’s EDL.

For more information about the origins of Privacy by Design, please see my paper “Privacy by Design,” available online at http://www.ipc.on.ca/images/Resources/privacybydesign.pdf
I realize that incorporating an on/off switch into the EDL prior to the government’s June 2009 deadline is not possible. In the meantime, for those who choose to obtain an EDL, I would caution you to be aware of the privacy risks. Although the protective sleeve provided with the EDL is not a complete privacy solution, until there is an on/off switch incorporated into the EDL, everyone should use it.

The Ontario government will issue a protective sleeve with the EDL, saying it “will prevent anyone from reading the RFID information unless you remove the card from the sleeve.” However, experiments conducted on Washington State’s EDL show that even while encased in a sleeve, the information on the EDL’s RFID tag may be read. Specifically, it was shown that a sleeved EDL held in one’s hand could be read at 27 cm. Researchers also found that in a crumpled sleeve an EDL in a back pocket wallet could be read at 57 cm.

Even if sleeves could successfully block reader access completely, there are two remaining problems. First, there is no guarantee that individuals will actually use the sleeves. The results of an EDL pilot in British Columbia, Canada, show that some individuals rarely used the sleeve, because the sleeved EDL did not fit in the slits found in virtually all wallets, or the sleeve was not convenient to use.

Second, most of the time, Ontarians will be using the EDL as a driver’s licence or government-issued photo identification document, while driving around Ontario – having nothing to do with crossing the U.S. border. Whenever someone takes their licence out of the sleeve for non-border-crossing purposes, the EDL then would be vulnerable to surreptitious, unauthorized reading.

The support for an on/off switch for the EDL has been gaining momentum and public interest since I first raised it last year. A University of Washington study presents various technical and procedural improvements to the EDL, including adding an on/off switch to the card. Also, a 2009 MIT publication references the work of Professor Avi Rubin from Johns Hopkins University, who agrees that an on/off switch could be added to EDLs.

---

2 Enhanced Driver’s Licence (Background and FAQ), online: Ontario Ministry of Transportation http://www.mto.gov.on.ca/english/dandv/driver/enhancedcards.shtml
5 E. Naone, “RFID’s Security Problem Are U.S. passport cards and new state driver’s licenses with RFID truly secure?” MIT’s Technology Review (January/February 2009), online: http://www.technologyreview.com/computing/21842/?a=f
I continue to advance the privacy-enhancing solution of adding an on/off switch into the EDL. My Office’s research indicates that there is no legal impediment that precludes an on/off device meeting the Western Hemisphere Travel Initiative (WHTI) criteria, as prescribed by the U.S. Department of Homeland Security.

These efforts are intended to provide Ontarians with a technology to protect their privacy if they choose to use an EDL. I sincerely hope that an on/off switch is made available for use in the near future with Ontario’s EDL. Such an innovative privacy-enhancing addition could give Ontario first mover advantage by turning the EDL into a made-in-Ontario transformative technology that delivers both security and privacy.

Stay tuned!
The Commissioner’s Remarks to the Standing Committee of the Legislature of Ontario Regarding Bill 85, to Create an Enhanced Driver’s Licence

October 2008
Introduction

I would like to begin by thanking the members of the Standing Committee on General Government for the opportunity to make a presentation today during its review of Bill 85, commonly referred to as the Photo Card Act, 2008.

As Ontario’s Information and Privacy Commissioner, my mandate encompasses many responsibilities. Of these, I believe that providing counsel on the privacy implications of proposed legislation or sweeping technological changes to government is one of my most important duties. I also believe it is vitally important to be practical in the protection of privacy, and ensure that the right information reaches the public. Unless the public is informed of what the privacy issues are – and the associated concerns – these issues may surface only after the fact, when it may be too late. The public needs to understand the implications of this new program and legislation in order to make an informed choice if they decide to apply for one of these cards.

The primary purpose behind this proposed Bill is to enable the government to issue an enhanced driver’s licence, which I’ll refer to as an EDL, which is intended to serve as an alternative to a passport, solely for the purposes of entering the United States. In addition, the Bill provides the government with the authority to issue new photo cards for those who do not, or cannot, hold a driver’s licence – such as people who have a visual impairment. Such photo cards are available in virtually all other provinces. Bill 85 makes these available in Ontario and also allows the government to enhance them to serve as an alternative to a passport, when travelling to the United States – parallel to an EDL.

I further understand that the entire Western Hemisphere Travel Initiative, which I will refer to as WHTI – as it is commonly called, has grown out of security concerns following the events of 9/11. As an individual citizen, I certainly understand people’s fears relating to terrorism. However, as Commissioner, I also fear the potential loss of our freedoms, especially over privacy, which forms the basis of all of our freedoms.

In the days and months following 9/11, many people, especially those in the United States, were hesitant to speak out on behalf of privacy for fear of it being viewed as unpatriotic. I remember vividly, days after 9/11, in response to a call from the
CBC seeking my “position” on the event, I issued a position paper posted jointly to our websites, headed: Public safety is paramount, but balanced against privacy. The position I took was that, of course, we had to protect public safety but, and a very important “but,” we also had to ensure that any security measures undertaken were real and not illusory. They had to be necessary and effective. We couldn’t just give up our privacy, our freedom, for the mere appearance of security – it had to be real. I argued that our search for safety and security could not come at the expense of privacy. This would be a fundamental error. Forfeiting our privacy in the pursuit of security is simply too high a price to pay – since privacy is at the heart of freedom.

Having said that, I want to make clear that my purpose here today is not to oppose Bill 85, but rather to share some concerns I have with the legislation. I also want to state for the record that I am not opposing the government’s commitment to introduce an alternative border crossing document to the Canadian passport. I will remind you how this came about and is actually the lesser of two evils. I just want to make sure that privacy is built into the program.

Let me first tell you that over the last year, my Office has developed a good working relationship with the Ministry of Transportation (MTO), and Ontario’s Intergovernmental Affairs and Cabinet Office, who have been keeping my Office informed of the implications of WHTI and Ontario’s plans to implement an alternative border crossing device acceptable to the U.S. government.

My office has been proactive in advancing the public’s understanding of this project. This past summer, I had the opportunity to jointly co-host, with Professor Andrew Clement, of the University of Toronto, a public forum on the privacy and security issues involving the EDL. We heard arguments from members of both sides of the debate, including from the University of Toronto’s Identity, Privacy and Security Initiative, an excellent program, as well as representatives from both the provincial and federal governments, and consumer and citizen interest groups such as the Consumer Council of Canada, the Binational Tourism Alliance, and the Canadian National Institute for the Blind. This multi-stakeholder input was very helpful in clarifying various elements of the EDL program.

Moving forward, I would now like to give you an overview of my privacy concerns regarding Bill 85.

After careful study, we noticed that Bill 85 was missing several privacy principles commonly included under internationally recognized Fair Information Principles. While each of these principles is detailed in my submission, I will discuss just one here, that speaks to the question of “accountability.”
Accountability – Openness and Transparency/Public Consultation

Openness and transparency are key to government accountability, especially when the government serves as the custodian of a significant amount of personal information on its citizens. My concern here is that Bill 85 leaves crucial matters affecting the privacy and security of Ontarians either to the discretion of government officials, or to be later prescribed by regulation, without any requirement for public notice or comment.

These matters are not defined in Bill 85 and do not list the specific personal information to be collected, used or disclosed by the government or details, such as:

- The information to be contained on the photo card;
- The security and other features that may allow the photo card to be used for travel purposes;
- The information that the Ontario government will collect from municipalities and other provincial, territorial and federal government departments and agencies, which is too broad;
- The information that the Ontario government will provide to municipalities, and other provincial and federal government departments and agencies, is not clear;
- The contents of information-sharing agreements; and
- The requirements for being issued a photo card.

Under these circumstances, in order for transparency and accountability to be achieved, the regulation-making powers provided for under Bill 85 must allow for public consultation before a regulation is enacted. This would not be the first time in Ontario that such consultation was set out in legislation. Other instances include the Personal Health Information Protection Act, the Environmental Bill of Rights, and the Occupational Health and Safety Act.

As government officials and public servants, I feel that we must provide an opportunity for the people of Ontario to voice their thoughts and views regarding a decision that may impact their lives. In my recommendations, I have suggested specific wording to accomplish this based on the wording contained in Ontario’s Personal Health Information Protection Act.

With regards to government accountability, I would also like to state that Bill 85’s provisions relating to photo-comparison technology should be made more “transparent.” It is my understanding that the proposed technology will utilize a facial recognition software application that will convert a photograph, as has appeared on our driver’s licence for many years, into a biometric template, to allow comparisons.
within the Ministry’s database of driver photos. The government must make assurances that any biometric collected, even one that the public is accustomed to and that has been collected for some time, will only be used internally, and solely for the purpose of verifying the identity of card holders. Placing strict controls on its use is crucial.

In the remaining time, I am going to devote my comments to two important areas: verification of citizenship information, and Radio Frequency Identification technology, or RFIDs. First, let me briefly discuss the issue of citizenship verification.

Citizenship Verification/Duplication of Databases

Earlier this year, I went so far as to issue a press release to make the public aware of one of my biggest concerns regarding the security risks associated with the proposed EDL program. Provinces are being asked to verify the citizenship of applicants for the purpose of the EDL program (and the enhanced photo card for non-drivers). Applicants will have to provide proof of Canadian citizenship to the Ministry of Transportation, complete a questionnaire (with questions such as “At the time of your birth, was one of your parents a foreign diplomat, consular officer or representative or employee of a foreign government recognized by the Canadian Government?” “Did one of your parents ever renounce or give up their Canadian citizenship before February 15, 1977?”), and undergo an in-person interview.

I respectfully asked that the federal government – the Government of Canada – securely provide citizenship information on naturalized citizens (those not born in Canada) to Ontario to avoid the need to recreate a duplicate process of verifying citizenship for Canadians who apply for an EDL.

This isn’t something new. We have several precedents – other examples of secure information sharing between our federal and provincial governments. For example:

- Ontario’s GAINs program, which receives tax status information on individuals from the federal Canada Revenue Agency, who possesses that information.

I initiated a dialogue with The Honourable Stockwell Day, Minister of Public Safety, responsible for national coordination of the EDL program, some time ago, to request that the Department of Citizenship and Immigration (CIC) provide the citizenship information they hold to provinces that request it.

Further, in early correspondence with Ontario’s Deputy Minister of Transportation and the Deputy Minister of Intergovernmental Affairs, I noted the fact that when it comes to responsible information management, the practice of data minimization should always prevail, meaning, don’t collect any new information – new personal data – if you don’t have to. Requiring provinces to build their own database of citizenship information from scratch – in effect, re-inventing the wheel, when the
The Commissioner’s Remarks to the Standing Committee of the Legislature of Ontario Regarding Bill 85

federal government already has this information – needlessly adds to privacy and security concerns, not to mention the unnecessary costs of a cumbersome and highly duplicative process. Simply put, the federal government does not need to waste valuable time and resources, not to mention our taxpayer dollars, by duplicating existing government resources.

Creating a mirror database of citizenship information already held by the federal government could very well serve to propagate identity theft and add to the potential of unintended consequences, of error and inaccuracy, that would arise in the process of recreating existing information. And lest you think that this is a simple “yes-no” answer for citizenship, I assure you, it is not. The database would apparently need to contain the answers and notes to a lengthy in-person interview for each applicant. And it may not end there. If the interview questions reveal a complicated situation, the matter is then to be forwarded to the federal government in any event, resulting in further duplication, cost and privacy risk. This is no simple matter. Let’s not complicate it further.

And let me be clear – I know this is a federal issue, not the doing of the Premier or Minister of Transportation. But regardless of the fact that it was created by the federal government, it must be resolved now. The federal government already has this information. It has the ability to easily verify the citizenship of naturalized Canadians, and securely provide that information to a province, such as Ontario, upon request. This is clearly a more privacy protective and cost-effective model – a “win/win” scenario – more privacy and security; lower cost.

Now, let me turn to another area which I feel is a very critical aspect of Bill 85 – the use of Radio Frequency Identification technology, or RFIDs.

**RFID Technology**

For those of you who may not be familiar with RFID technology, let me give you a very brief introduction to the topic, and I mean brief.

RFID is a generic term for a variety of technologies that use radio waves for purposes of automatic identification, consisting of two integral parts: a tag, and a reader – think “bar code on steroids.”

There are two main types of RFID tag: active or passive, which differ depending on whether they have their own power system. Passive tags have no power source and no on-tag transmitter.

Finally, you need to know that RFID tags are activated by readers, which, in turn, are connected to a host computer. In a passive system, the RFID reader transmits a signal via the airwaves that “wakes up” the tag by powering up its chip, which in turn enables it to transmit data.
Privacy by Design

I have spent many years working in this field, trying to secure privacy within RFID technology, and my Office has produced three papers and a set of practical guidelines on the subject. I am not opposed to the use of RFID tags across the board — indeed, they can have many benefits. But, like all information technologies, they need to have privacy issues baked into them early in the design of these systems. I call this “privacy by design,” a term I first developed in the early ‘90s, which ensures that privacy does not become an afterthought, because it has been built right into the system.

Tagging things in areas such as the supply-chain management process or taking an inventory of assets, poses no risk to privacy. Tagging, however, can raise concerns because of the relative permanence of the tag, the nature and amount of data collected, and the strength of the data’s linkage to personally identifiable individuals, in addition to the sensitivity of the data involved. Once you have the possibility of data linkage, allowing for individuals to become identifiable, that’s when privacy concerns arise.

Here’s how this relates to Bill 85 and the EDL program

Currently, U.S. Customs and Border Protection (CBP) uses RFID technology on its trusted or registered traveller programs – such as NEXUS – at designated land border sites, in order to “expedite the processing of pre-approved, international, and low-risk commercial and commuter travelers crossing the border.” The Department of Homeland Security requires that any approved border travel document carry RFID tags.

Arlene White, Executive Director for the Bi-national Tourism Alliance, a not-for-profit trade organization created to support tourism in cross-border regions shared by Canada and the United States, spoke at the summer EDL Forum we held, about these border communities and their strong support for this program. She emphasized their desire to ensure the smooth flow of traffic at their borders which, in her view, would not be possible without this RFID technology.

Let me now give you some sense of what all of this means with regards to privacy and security.

A fundamental characteristic of all RFID technologies is that they are wireless. This means that any data contained on the chip – in this case, a unique index number which is stored on the embedded RFID chip – is transmitted through an RFID reader to a database of information. This number serves as a pointer to the individual’s personal information contained in the database, needed for the completion of this process.

Now, there are well-known privacy and security vulnerabilities associated with RFID technology that are commonplace, and apply to any RFID-enabled identification card and information system. Briefly, the top three are:
**Skimming** – which occurs when an individual with an unauthorized RFID reader gathers information from an RFID chip without the cardholder’s knowledge; remember, the RFID is emitting radio frequencies that can be picked up by any readers in the area, authorized or unauthorized;

**Eavesdropping** – which occurs when an unauthorized individual intercepts data, using an authorized RFID reader;

**Cloning** – which occurs when the unique information contained on the original RFID chip is read or intercepted, and its data are duplicated.

These vulnerabilities could lead to a host of undesirable consequences such as unauthorized identification, identity theft and most serious, the surreptitious tracking and surveillance of individuals – say good-bye to privacy.

In response to some of these concerns, you will be told that the RFID Gen2 standard, to be used for the EDL, does not include any personally identifiable information, only a unique number linking the cardholder to his or her record in a database, so no privacy concerns, right? WRONG! Just think of a social insurance number, a passport number or a driver’s licence number – while each of these identification numbers may appear to be “just a string of numbers,” “of no use to anyone,” when linked to personally identifiable information, each can be subject to abuse, by unauthorized parties or used for unintended purposes that may cause real harm to real people. Just think of identity theft as a case in point.

So a number, when uniquely linked to an individual, is not inconsequential – it’s not just a meaningless number. It points to real, personally identifiable information, that may then be subjected to abuse.

Regardless of the contents of the data stored on the chip, if that data is both static and accessible, via an unauthorized reader – or network of readers – then the cardholder’s identity may be ascertained, and the individual can then be tracked, without his or her knowledge. Even if the data on the card cannot be associated with existing personal information about the cardholder, it could be used to collect information in the future. I know this sounds like wildly futuristic scenarios, but I assure you, it’s not that far off.

In the here and now, identity theft is on the rise and is now considered by both Canadian and American law enforcement agencies to be the fastest growing form of consumer fraud in North America – much of which is due to organized crime having entered into the scene, en masse.

Currently, the suggested method for allowing cardholders a measure of privacy and security is to provide them with an “electronically opaque” sleeve, called a Faraday Cage, which would prevent communications to and from the RFID chip,
if the card was encased in the sleeve – some call it the Dorito Chips bag. Aluminum foil also does the trick.

But this is not a sufficient answer. The cardholder must take on an added inconvenience, but must also remember to place his or her card into such a device. It won’t happen. They won’t remember to do it, or bother to do it, or want to do it. They’ll want the ease of slipping their licence into their wallets, just like they do now.

This proposed protective sleeve, when offered as the only privacy measure, would realistically mean that the card would allow, by default, the collection of stored data by unauthorized RFID readers, until the cardholder remembered to place the card in the sleeve. This solution is only protective when the individual remembers to place the card in the sleeve – otherwise, the reading of cards becomes free and clear.

Even leading researchers such as Sophia Cope, staff attorney and a fellow at the Center for Democracy and Technology, agree that this method is hardly sufficient. In her testimony before a Senate Committee on the implementation of the REAL ID Act and the Western Hemisphere Travel Initiative, Ms. Cope stated that privacy risk mitigation measures such as the Faraday sleeve, “improperly place the burden of privacy protection on the citizen. Moreover, they offer no protection in light of the fact that the EDL will be used in many circumstances where driver’s licenses or ID cards are now required, including in many commercial contexts, where individuals will be taking their cards out of the protective sleeve, thereby exposing their data to all the risks we have described above.” In Ontario, people often use their driver’s licence when asked for a government-issued photo ID – to vote, to open a bank account or apply for a credit card.

As the RFID standard chosen for this project will respond to any reader query, I feel that the card must have some means of preventing it from being read when not required, when used for multiple purposes other than border crossing – a better solution than the proposed sleeve is needed.

So the way that I always proceed is to go off and look for solutions. One of the best options that I’ve heard of would be to give the cardholder the option of physically verifying the selected transmission setting, meaning adding the equivalent of an “on/off” switch to the RFID, which can be incorporated directly onto the card.

And I am not proposing this based on “yet-to-be-developed” technology. Several groups are developing this. At MIT, The Media Lab has already patented and prototyped an “on/off switch” for the RFID tag that can be incorporated directly into a card, allowing the cardholder to determine when and where their information will be transmitted.

So has another company based in the U.K. – Peratech, a company that has advanced this even further, having developed an on/off switch using Quantum
Tunneling Composites technology. Its founder and CTO David Lussey advised me that, "Peratech’s technology is readily available under license for the application of acting as an on/off switch on an RFID driver’s license. It has been fully proven to work reliably in the typical hot-lamination manufacturing process used by all the major RFID card manufacturers. And it is just a matter of cents, not dollars, that we are talking about." This is indeed a very promising prospect.

There’s also another company in the United States – Root Labs – which is working on a similar switch that will be placed on transponders used by San Francisco Bay highway toll users.

I brought together our government and the vendor selected to produce EDLs in Ontario, hoping to advance this very promising technology, which I believe should be seriously considered for EDLs here in Ontario. I felt that it was necessary to bring them together, with the goal of advancing the feasibility and development of this promising technology. In fact, a senior executive, from the government’s selected vendor, told me, "We are aware of the developments of new and emerging technologies that provide the means to personally control RFID transmission of data with an ‘on/off’ switch on a card, such as Peratech’s QTC technology. Furthermore, Giesecke & Devrient (G&D) is working diligently on the development of our own technologies and assessment of third-party technologies to enhance RFID functionality, security and also privacy."

Great – the more options available, the better. Stay tuned.

Privacy by Design

Let me shift gears now and give you some perspective, by way of background, on privacy and technology. Since the early ‘90s, I have been advancing the idea that technology has the ability not only to provide good security but also to protect our privacy. In 1995, I put forward the view that technology can liberate us from the “zero-sum” trap of having to sacrifice privacy in order to have security. But in order to do this, we have to move forward toward a “positive-sum” paradigm. We cannot view privacy and security as polar opposites. In this new positive sum “win-win” scenario, privacy and security can both co-exist because technology is enlisted to protect privacy and safeguard personal information through the use of privacy-enhancing technologies (PETs). When applied to technologies of surveillance, PETs can serve to transform these technologies into ones that are protective of privacy, hence my new term, “transformative technologies.” I say transformative technologies because I believe that technology has evolved to the point where it now has the ability to protect our privacy while performing whatever functionality it was designed to perform, but only if privacy is built directly into the architecture of that technology at the developmental stage. As I’ve said, I
call this “privacy by design,” and it is my mantra. Privacy can either be achieved through the use of PETs, by eliminating or minimizing the collection of personal data, or by preventing the unnecessary and undesirable uses of personal data, all without losing the functionality of that technology. And this can be achieved by keeping privacy in mind and embedding it into the design and architecture of new technologies – Win/Win, not either/or!

And so, in the spirit of the above, I recommend the following regarding the use of RFID technology, in the EDL.

First, I would like to recommend that any use of Radio Frequency Identification technology comply with the RFID guidelines set by my Office (and I have brought along a copy with me today, for your convenience.)

Second, and most important, I recommend that the Ministry work with the selected vendor to pilot test the privacy-enhancing technology of adding an on/off switch for the RFID tag embedded in the card. This will enable far greater protection of the card, when not being used for border-crossing purposes.

Conclusion

Let me conclude by sharing a motto that my Office developed some time ago, and follows religiously. I call it the 3C’s: Consultation; Collaboration; and Co-operation. This philosophy, I believe, represents the ethos of my Office and this is the attitude I carry into my work regarding the EDL program.

As I have stated, I am not opposed to the EDL program, but I do have concerns regarding privacy, which I feel must be addressed, based on the mandate given to me by the Legislature of Ontario – and I look forward to serving that mandate in the spirit of the 3C’s.

Thank you once again for providing me with the opportunity to appear before the Committee and for considering my Office’s comments on the Act. I am confident that, with our continued collaborative efforts, we will be able to appropriately address any outstanding privacy matters and to best serve the people of Ontario. In fact, we could develop the most privacy-protective EDL available anywhere in the world – another first for Ontario, and hopefully, one of many more to come.

Thank you.
Increase Airport Security Without Compromising Privacy:
Commissioner Cavoukian Makes the Case for the Use of “Privacy Filters”

March 2009
Increase Airport Security Without Compromising Privacy:

Commissioner Cavoukian Makes the Case for the Use of “Privacy Filters”

Whole Body Imaging (WBI) technologies – which have been described in the media as “naked scanners” – raise significant privacy concerns that must to be addressed, says Ontario’s Information and Privacy Commissioner, Dr. Ann Cavoukian. “These technologies, which are being deployed as a voluntary passenger-scanning security measure in a growing number of airports around the world, pose a serious threat to privacy since they produce high-quality images of an essentially naked body beneath a passenger’s clothes.” But the risk to privacy can easily be mitigated through the use of a strong “privacy filter.”

The Commissioner released a white paper entitled Whole Body Imaging in Airport Scanners: Activate Privacy Filters to Achieve Security and Privacy, which outlines how the activation of privacy (or modesty) filters can reduce the amount of unnecessary personal details captured by WBI technologies.

“The choice is clear,” said Commissioner Cavoukian. “Whole Body Imaging technologies which incorporate privacy filters that render bodily images to mere outlines have great potential to provide privacy-protective security. This is how WBI can rise above its negative privacy connotations and became a Transformative Technology, delivering both security and privacy.”

This paper is the latest in a series of works that build on the Commissioner’s Privacy by Design concept, where privacy-enhancing technologies are designed directly into new technologies, right from the outset.

Whole Body Imaging technology involves a process by which various imaging techniques are used to scan and create a full body (2- or 3-dimensional) image of an individual, including the surface of the skin and objects on, but not in, the body. Currently, the scan is conducted using one of two technologies:

- Millimetre-wave, which uses non-ionizing radio frequency energy in the millimetre-wave spectrum to detect energy reflected from the body to construct a three-dimensional body image. (The most widely used WBI technology); or
- Backscatter, which uses the reflections from a low-intensity X-ray beam to construct a two-dimensional image.
Both of these technologies are capable of producing highly detailed images of the human body. Fortunately, a number of algorithms serving as privacy (modesty) filters have been developed to greatly reduce the level of personal detail in the images displayed to screeners, while simultaneously highlighting any concealed objects covertly carried on the person.

Governments and public officials should ensure that vendors of WBI incorporate a privacy filter that obscures personal bodily details, and that it is activated when the technology is deployed.

In addition to ensuring that privacy algorithms are applied to WBI images, other design and operational factors are also critical to any overall privacy assessment, stressed the Commissioner. “In particular, there must be a complete prohibition against any retention or transmission of routine (threat-free) images, in any format.”

“Ultimately, it comes down to public confidence and trust that the minimum information required is captured by system operators and used to make decisions affecting travellers,” said Commissioner Cavoukian. “Clear and transparent rules affecting system design and operation, supported by credible assurance methods, will help enormously.” In other words, if no hidden weapon or concealed objects are found during a scan, then no information should be retained – data minimization at its best.
Whole Body Imaging in Airport Scanners: Activate Privacy Filters to Achieve Security and Privacy

March 2009
Whole Body Imaging in Airport Scanners: Activate Privacy Filters to Achieve Security and Privacy

Whole Body Imaging (WBI) technologies are being deployed as a passenger scanning measure in a growing number of airports in order to complement, and at times replace, other security technologies such as metal or explosive detectors.\(^1\)\(^2\) Described in the press as a “naked scanner,” these technologies have the ability to produce high-quality images of the naked body beneath a passenger’s clothes.\(^3\) Improved airport security, however, need not come at the expense of privacy – both may be achieved together in a positive-sum (not zero-sum) manner. This paper will describe the possible means for WBI to rise above its negative privacy connotations and become what we are calling, a Transformati ve Technology. We believe that the privacy-invasive potential of Whole Body Imaging must be squarely addressed in the design phase of the technology, as well as in its deployment and use, with attention to physical privacy and adequate privacy processes.

Transformative Technologies

In 1995, the Ontario Information and Privacy Commissioner (IPC) and the Dutch Data Protection Authority coined the acronym PETs, for Privacy-Enhancing Technologies. This term refers to coherent systems of information and communication technologies that strengthen the protection of privacy in information systems by preventing the unnecessary or unlawful collection, use, and disclosure of personal data, or by offering tools to enhance an individual’s control over his or her data. PETs are the technological embodiment of the universal privacy principles contained in fair information practices.

In 2008, my office extended the idea of PETs to PETs Plus\(^4\), creating the new concept of Transformati ve Technologies\(^5\). Dissatisfied with the “zero-sum” paradigm of security vs. privacy, in which gains in security are met with corresponding losses in privacy (and vice versa), we embraced the notion of a positive-sum paradigm,

\(^2\) http://en.wikipedia.org/wiki/Puffer_Machine
\(^4\) Cavoukian, Ann, Ph.D., Moving Forward from PETs to PETs Plus: The Time for Change is Now at: www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=834
\(^5\) Cavoukian, Ann, Ph.D., Transformative Technologies Deliver Both Security and Privacy: Think Positive-Sum not Zero-Sum, at: www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=758
in which all parties can benefit from technological advances. In this paradigm, privacy protections are incorporated into security technologies from the outset, hence the Commissioner’s term, “Privacy by Design.” Applying a PET to a surveillance technology, while maintaining the goal of a positive-sum paradigm, can create a “Transformative Technology” because it can, in effect, transform an otherwise privacy-invasive technology into a privacy-protective one.

**Positive-Sum Paradigm + Privacy-Enhancing Technology = Transformative Technology**

Virtually any privacy-invasive surveillance or security technology can be turned into a *Transformative Technology*, and Whole Body Imaging is no exception.

**Whole Body Imaging**

Whole Body Imaging technology involves a process by which various imaging techniques are used to scan and create a full-body (two- or three-dimensional) image of an individual, including the surface of the skin and objects on, but not in, the body. Currently, the scan is conducted using one of two technologies:

**Backscatter**, which uses the reflections from a low-intensity X-ray beam to construct a two-dimensional (2-D) image, or

**Millimetre-wave**, which uses non-ionizing radio frequency energy in the millimetre-wave spectrum to detect energy reflected from the body to construct a three-dimensional (3-D) body image.

The stated goals of the use of WBI technologies for passenger screening are twofold: first, such imaging is reported to be superior in its ability to detect both metallic and non-metallic threat objects; second, airport authorities believe that this procedure will be the preferred choice to physical pat-downs or strip searches for individuals undergoing security screening.

A number of trials have already been undertaken to evaluate the effectiveness of WBI technology for secondary passenger screening at airports. In the United States, WBI was tested at Phoenix, Boston, Chicago, Las Vegas, Kansas City, Los Angeles, Miami, Tampa, and at JFK Airport in New York, among others. The U.S. Transportation

---

6 “Privacy by Design” is a term coined in the ’90s by Ontario’s Information and Privacy Commissioner, Dr. Ann Cavoukian, in an effort to enlist the support of technology to protect privacy, rather than encroach upon it. For more details, see her *Privacy by Design* paper, at: www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=835 or go to: www.privacybydesign.ca

7 Although both types of scanning technologies are effective at detecting aviation threat objects, it is predominantly millimetre-wave rather than backscatter systems that are being deployed at airports. The main reasons for this predominance appear to be twofold: (a) preference for using radio waves instead of X-rays and (b) faster passenger processing by the millimeter-wave machines. Both systems, however, can produce highly detailed and identifiable images of the naked body, absent the use of strong privacy filters.
Security Administration (TSA) intends to deploy 120 machines in 23 locations nationwide by the end of 2009. Similar trials were undertaken in India (New Delhi), Australia (Sydney, Melbourne and Adelaide), Japan (Osaka), Russia (Moscow), the Netherlands (Amsterdam’s Schiphol) and at London’s Heathrow Airport in 2004.

After testing WBI in 2006, the organization responsible for security at India’s airports – the Central Industrial Security Force (CISF) rejected the use of the machines. The CISF claimed that the images the machines produced were too revealing and would offend passengers, as well as embarrass their security officials.

Scrutiny is increasing. In September 2008, the European Commission, part of the European Union’s (EU) executive branch, proposed adding the machines to a list of security measures used in EU airports, saying that the scanners would not be used routinely on passengers, and would provide a less intrusive alternate to strip-searching. The proposal was withdrawn after the European Parliament ruled that the scanners “have a serious impact on the fundamental rights of citizens” and voted overwhelmingly for additional study on the privacy and safety implications. The Commission said it will continue examining how the scanners can be used in consultation with the European Data protection Supervisor (EDPS), the Article 29 Working Party and the Fundamental Rights Agency, and “is now in the process of drawing up a package of rules for how the scanners will be deployed.

Meanwhile, the U.S. TSA has proceeded to Phase 2 of its deployment strategy, that is, using WBI for primary screening. On January 19, 2009, USA Today reported that, “For the first time, some airline passengers will skip metal detectors and instead be screened by body scanning machines that look through clothing for hidden weapons.” This will be taking place at Tulsa International Airport, followed by airports in San Francisco, Las Vegas, Miami, Albuquerque, and Salt Lake City. “Passengers at the test airports will be instructed to go through the new scanners. Anyone who doesn’t want to go through will be allowed to refuse and instead go through a metal detector and receive a pat-down.”

---

8 www.tsa.gov/approach/tech/body_imaging.shtm
9 www.timesonline.co.uk/tol/news/uk/article504009.ece
   Germany rejects full-body scans at airports, CBC News, October 24, 2008 at: www.cbc.ca/world/story/2008/10/24/germany-xray.html
In July 2008, the Canadian Air Transport Security Authority (CATSA) began a seven-month trial of millimetre-wave scanning technology for voluntary primary screening of passengers at Kelowna International Airport.14

**Technology: Obfuscation**

By themselves, both backscatter and millimetre-wave technologies produce highly detailed images, as illustrated by Figures 1 (at left), 2 and 3 (below).

This has led to the popular conception of WBI as a “virtual strip search.” Developers and users of these technologies have recognized this as an issue that must be addressed. A number of algorithms or privacy (“modesty”) filters have been developed with the goal of reducing or eliminating the level of personal detail contained in the images displayed to screeners, while simultaneously highlighting objects carried on the person. Thus, a wide range of potential images may be presented to screeners, ranging from detailed and identifiable to generic and unidentifiable.

Figure 1, above, is a widely distributed image of the director of the TSA’s security laboratory, who had consented to having her body X-rayed by the “backscatter” scanner at the U.S. Transportation Security Administration in 2003.15 This image demonstrates a raw, unfiltered backscatter image with no privacy filter applied.

Figures 2 and 3, to the right, are images created by millimetre-wave technology, which produce holographic black and white silhouettes. In the first frame a woman stands in standard screening pose, that is, legs apart with hands held over the head; in the second, a man is holding a half-filled bottle of water16. Privacy can be protected by using system options that display obfuscated images (e.g., by blurring facial features [Figure 2] and private areas [Figure 3].)

---


16 Photos by L-3 Communications as provided to Corrections.com and accessed at: [http://picasaweb.google.com/correctionsconnection/MillimeterWaveTechnology#5178699965699051458](http://picasaweb.google.com/correctionsconnection/MillimeterWaveTechnology#5178699965699051458)
Although both types of scanning technologies are effective at detecting aviation threat objects, it is predominantly millimetre-wave rather than backscatter systems that are being deployed at airports. The main reasons for this predominance appear to be twofold: (a) preference for using radio waves instead of X-rays; and (b) faster passenger processing by the millimetre-wave machines. Both systems can, however, produce highly detailed and identifiable images of the naked body, absent the use of strong privacy filters.

**Millimetre-Wave Privacy Algorithms**

In 2002, the IPC became aware of research undertaken by the U.S.-based Pacific Northwest National Laboratory (PNNL) with regards to privacy and 3-D body scans. In conjunction with their work on the millimetre-wave scanner (the “Personal Security Scanner”), the PNNL’s research team recognized that a natural objection to the adoption of this technology was the potential for the display of body details. They thus developed a privacy algorithm whose goal was to “… eliminate from the imagery, all human features that may be considered too intrusive.”

The privacy algorithm initially developed was based on a technology called “speckle detection.” The researchers found that plastics, ceramics, and other dielectric (i.e., non-conducting) materials are partially transparent to millimetre-wave insulation. This leads to a speckled texture in the scanned image, which appears visually as a granulated segment where the threat is located. Human skin, on the other hand, appears with a very smooth texture in millimetre-wave scans, with little pixel-to-pixel variation. Taking advantage of this difference, the researchers developed a neural network-based algorithm that examined various segments of the image for this granular texture, performing a series of post-processing tasks on “speckled” segments to reduce noise and false positives. It was determined that this algorithm was as effective at identifying threat objects as were trained human examiners who viewed the same images. Once threat objects were determined, the PNNL’s algorithm was able to indicate their locations in a number of ways, including on a 3-D rendering of a generic human form, which is especially important to this discussion.
Figure 4 (at left) illustrates the application of privacy-enhancing morphological edge and gradient detection software algorithms, developed by PNNL researchers, applied to WBI holographic millimetre-wave images. This technique goes far beyond simply masking the face and the genitals – it obscures the personal details associated with the entire body. PNNL researchers also developed other approaches to obscuring passenger image details.

In 2008, the IPC contacted the PNNL researchers, inquiring about any updates to their work. We were informed that PNNL privacy research in this area had been acquired in 2002 by Safeview, developers of “advanced technologies for the protection of people and property,” and later in 2006 by L-3 Communications, marketers of ProVision Checkpoint millimetre-wave passenger scanning technologies. However, it remains unclear what use, if any, L-3 Communications have made of PNNL’s privacy algorithms. The L-3 ProVision Whole Body Imager FAQ states only that “[p]rivacy can be … protected by using system options that allow for further blurring of facial features and blurring of private areas.” In conversations with L-3, they indicated they had no plans to incorporate this innovative privacy algorithm into their scanners.

Similar privacy-enhancing options are offered by Rapiscan Systems WaveScan 200 millimetre-wave scanners, sensors for which, according to the company, “do not image anatomical details, thus protecting privacy.”

Other laboratories have also been working on the development of privacy algorithms. Researchers, working at Carnegie Mellon’s CYLAB, have developed a means of blurring or making transparent “sensitive” areas of the human body, rather than removing all the details. This is accomplished by creating a detailed understanding of intrinsic human proportions, and using this data to limit the algorithmic search area for head, chest, and genital regions; once these areas are identified, various blurring and/or transparency filters can be applied.

---


21 Ibid, (See also #18 and U.S. Patent 7365672 – Detection of a concealed object at: www.patentstorm.us/patents/7365672/description.html)

22 www.dsxray.com/pdf/ProVisionFAQSEPT08.pdf


Backscatter Privacy Algorithm

Privacy algorithms for backscatter images, which are two-dimensional (as opposed to the 3-D images of millimetre-wave scanning), endeavour to reduce human features to the level of a “chalk outline.” The system “creates an image that looks like a chalk outline of the passenger with threats outlined, but does not reveal facial features” (see Figure 5 below), according to American Science and Engineering (AS&E), manufacturer of the SmartCheck Z Backscatter Personnel Screening System used by the Transportation Security Administration. Additionally, company information notes that “the SmartCheck systems installed at JFK, LAX and Phoenix Sky Harbor cannot store, export, print or transmit images.”

Figure 5, below, shows a sample backscatter image from an AS&E machine, run through their privacy filter. Outline images such as these are far more privacy-protective and thus preferable to the image shown in Figures 1, 2 and 3.

Activate the Privacy Filter

Governments, public officials, and vendors of WBI must ensure that privacy filters obscuring bodily details are available and activated, and that all personnel operating these scanners are trained in their use. When faced with the choice of having the image in Figure 1 vs. Figure 5 appear, I believe that most people would opt for Figure 5, which obscures all personal bodily details. Why wouldn’t governments select Figure 5, which only displays an outline of the physical form but yet clearly reveals any and all concealed objects? The choice is clear, and yet there has been very little discussion of the “privacy filters” available for use with Whole Body Image scanners. They represent a positive-sum, privacy-enhancing technology, that can be truly transformative in nature. But first, they must be used – we must ask that strong privacy filters, as illustrated in Figures 4 and 5, be installed and activated.

25 www.as-e.com/products_solutions/tsa_z_backscatter_pilot.asp
26 www.msnbc.msn.com/id/26408850/
27 Figure source from AS&E Inc. at: www.as-e.com/products_solutions/tsa_z_backscatter_pilot.asp
WBI and “Privacy by Design”

In addition to ensuring that strong privacy algorithms are applied to WBI technology, other design and operational factors, such as physical design and program practices, are also critical to a Privacy by Design approach.28

In particular, there must be a complete prohibition against any retention or transmission of the images in any format.29 This policy and practice may also require audits and other assurance methods in order to ensure compliance, thereby engendering public confidence and trust. Bruce Schneier, a security technology expert and noted author, said that the machines strike an “excellent” balance between privacy and security, but adds “the issue we’re worried about is whether they save the images.”30

Another important factor is who actually sees the WBI images, and when. Airport authorities in Canada and the U.S. have created separate image viewing rooms (in remote back rooms), where security personnel cannot see the scanned passengers before or after the scans, and do not have access to passenger details. These personnel are also banned from bringing photographic devices (including cellphones) into the viewing area and are prohibited from connecting storage or communication devices to the machine. We applaud this approach.

When security screeners in the remote “backroom” notice an anomaly or detect a potential threat in the WBI images, they can communicate this information in real time to “front line” screening personnel (who are actually out front, next to the passengers) through a different graphical interface, such as the one shown at left in Figure 6, developed by CATSA for use in Kelowna. The TSA has developed a similar interface for frontline screeners. Here, you can see that areas of the body requiring further inspection by front-line screeners are highlighted on a generic body outline, with no physical bodily parts actually seen. Additional information, if needed, can be shared between screeners via discreet radio communications. This is an excellent privacy practice that supports image obfuscation, and should go a long way towards alleviating the privacy concerns of passengers actually interacting with airport screening officials.

29 www.msnbc.msn.com/id/26408850/
We also note that participation in the system is voluntary and mainly used for secondary screening purposes at this time. However, as noted earlier, WBI is starting to be used for primary screening as well. Travellers who are uncertain or uncomfortable should have the complete freedom to choose not to submit to the image screening, without being required to provide a reason or being subjected to any penalty, and to opt instead for traditional metal detectors.

Ultimately, it comes down to public confidence and trust that the minimum information required will be captured by system operators and used responsibly to make decisions affecting travellers. Clear and transparent rules affecting system design and operation, supported by credible assurance methods, will go a long way in this regard.

**Conclusion**

Whole Body Imaging technologies that incorporate strong privacy filters – rendering bodily images to mere outlines, to front-line screeners (Figures 5 and 6), can deliver privacy-protective security. When combined with appropriate viewing, usage and retention policies, privacy algorithms that obscure personal details, while still allowing potentially threatening concealed objects to be revealed, will allow WBI implementations to satisfy security requirements without sacrificing (and perhaps enhancing) passenger privacy. We believe that this positive-sum paradigm can, and should be, the end goal of such airport security passenger screening technologies – security and privacy, not one at the expense of the other.
7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity

October 2006
7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity

Backdrop

The existing identity infrastructure of the Internet is no longer sustainable. The level of fraudulent activity online has grown exponentially over the years and is now threatening to cripple e-commerce. Something must be done now before consumer confidence and trust in online activities are so diminished as to lead to its demise. Enter the 7 Laws of Identity: could this be the answer? Read on.

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

Introduction

This paper recognizes and is inspired by the “7 Laws of Identity” formulated on an open blog by a global community of experts through the leadership of Kim Cameron, Chief Identity Architect at Microsoft.

The Office of the Information and Privacy Commissioner of Ontario is convinced that the “7 Laws” (a.k.a. “technologically necessary principles of identity management”) will profoundly shape the architecture and growth of a universal identity metasystem. The resulting “Identity Big Bang” will hopefully enable the Internet to evolve to the next level of trust and capability.

A universal identity metasystem will also have profound impacts on privacy since the digital identities of people – and the devices associated with them – constitute personal information. Care must be taken that a universal, interoperable identity metasystem does not get distorted and become an infrastructure of universal surveillance.

We have always advocated that privacy be built into the design and operation of information systems and technologies. We do this by applying the privacy principles expressed in the “fair information practices” in a systematic way. (See Appendix A.)

We are struck by the many similarities between the 7 Laws of Identity and the fair information practices. The two sets of fundamental principles are highly complementary and inform each other.
This document is the result of our “mapping” fair information practices over the 7 Laws of Identity to explicitly extract their privacy-protective features. The result, which we call the “privacy-embedded” Laws of Identity, is a commentary on the Laws that “teases-out” the privacy implications, for all to consider.

The privacy-embedded Laws of Identity are intended to inject privacy considerations into discussions involving identity – specifically, into the emerging technologies that will define an interoperable identity system.

We believe that privacy is woven through the 7 Laws and that when the Laws are applied, exciting new privacy options will become possible. However, there is nothing inevitable about privacy-enhanced identification and authentication options. An identity metasystem (described by the 7 Laws) is a necessary but not sufficient condition for privacy-enhancing options to be developed.

The missing ingredients are knowledge and desire. If privacy design options for identity systems can be identified and promoted, then it is possible that a universal identity metasystem will emerge that has built-in respect for privacy and data protection, before it’s too late.

Identity and Privacy
Identity and privacy are closely related. Generally speaking, when your identity is not known, you tend to have more privacy. When you pay cash for a coffee, your “identity” is that of an anonymous consumer. When you buy coffee with an anonymous pre-paid coffee card, your “identity” becomes that of a loyal patron. But when your name and address are linked to a pre-paid coffee card, all of your coffee purchases may be linked to you, as an identifiable individual. Information that can be linked to an identifiable individual is considered to be personal information.

Privacy refers to the claim or right of individuals to exercise a measure of control over the collection, use, and disclosure of their personal information. When your personal information is mishandled, your privacy interests are engaged.

Protecting and promoting individual privacy is a real challenge in an era of exponential creation, networking and duplication of data, most of which is identifiable in nature. There is more personal information out there than ever before, and most of it is controlled by others. Increasingly we have little control over our own information.

Identification requirements are everywhere, and increasing. We all have multiple identities that need to be managed. In the online digital environment, however, the identity challenges are greater, since identification demands are becoming more frequent. Increasingly, more and more granular information is being collected about us by others, and this data is being used in novel ways, for novel purposes – not all of which benefit the individual.
There is a growing disjunct with the bricks-and-mortar world where, for example, we can often demonstrate our identity (or credentials) by simply waving an ID document for visual inspection. But in the faceless online world, our identification “credential” is often recorded in databases, compared or collated with other data, and stored indefinitely for further uses.

At the same time, the identity of other entities online is becoming harder to verify. We often simply do not know who we are truly dealing with online, or how accountable they are with respect to the handling of our personal information.

**Digital Identity and Privacy: The Challenge**

For users and businesses alike, the Internet continues to be increasingly valuable. More people are using the web for everyday tasks, from shopping, banking, and paying bills to consuming media and entertainment. E-commerce opportunities are growing, with businesses delivering more services and content across the Internet, communicating and collaborating online, and inventing new ways to connect with each other.

But as the value of what people do online has increased, the Internet itself has become more complex, vulnerable, and dangerous. Online identity theft, fraud, and privacy concerns are on the rise, stemming from increasingly sophisticated practices such as “phishing,” “spear-phishing,” and “pharming.” Keeping track of multiple accounts, passwords, and authentication methods is difficult and frustrating for users. “Password fatigue” results in insecure practices such as re-using the same account names and passwords at many sites.

**The Need for Identity Management**

Identity management is a hot topic these days, but what exactly is it? The term does not have a clearly defined meaning, but technology-based identity management, in its broadest sense, refers to the administration and design of identity attributes, credentials, and privileges.

Identity management may be carried out centrally by others, as in the case of organizations that assign “log on” credentials to individuals to facilitate and control access to critical resources. When you leave the organization, your network identity and associated privileges are revoked by the system administrator. This is often called enterprise identity management or, more simply, provisioning. Centralized identity management may also occur beyond the enterprise, as when governments issue national identity cards for use in multiple scenarios, or in some online single-sign-on schemes such as Microsoft .Net Passport service.

Another form of identity management is “user-centric,” which seeks to place administration and control of identity information directly into the hands of individuals. Examples include network anonymization tools and form fillers that minimize
disclosure of personal information, or password managers that securely keep track of different credentials. In the real world, a wallet full of different identity cards is a user-centric form of identity management that allows individuals to choose the appropriate identity credential for the right purposes, such as a coffee card for coffee and a student ID card for discounts. Individuals can exercise control over how the information on those cards is read and used by others.

A third type of identity management, commonly referred to as “federated,” is a hybrid of the two. In such systems, one’s identity credentials are divided and spread out among many parties, with users controlling how they are shared and used. Some single sign-on schemes can work this way. The ability to authorize a government agency to share change-of-address information with other departments may be another. The risks to privacy can be offset by careful choice of trusted identity providers, and by greater convenience and efficiencies for users.

All three types of identity management systems are necessary, depending on the context. Identity is highly contextual. Consider that the identities held by a person in the offline world can range from the significant, such as birth certificates, passports, and driver’s licences, to the trivial, such as business cards or frequent user buyer’s cards. People use their different forms of identification in different contexts where they are accepted.

**Identity Is Contextual**

Personal information provided in different contexts will vary. Identities may be used in or out of context. Identities used out of context generally do not bring desired results. For example, trying to use a coffee card to cross a border is clearly out of context. On the other hand, using a bank card at an ATM, a government-issued ID at a border, a coffee card at a coffee shop, and a MS.Net Passport account at MSN Hotmail are all clearly in context.

In some cases, the distinction is less clear. You could conceivably use a government-issued ID at your ATM instead of a bank-issued card, but if this resulted in the government having knowledge of each financial transaction, many people would be uncomfortable. You could use a Social Insurance or Social Security Number as a student ID number, but that has significant privacy implications, such as facilitating identity theft. And you can use a .Net Passport account at some non-Microsoft sites, but few sites chose to enable this; even where it was enabled, few users did so because they felt that Microsoft’s participation in these interactions was out of context.

Numerous digital identity systems have been introduced, each with its own strengths and weaknesses. But no one single system meets the needs of every digital identity scenario. Even if it were possible to create one system that did so,
the reality is that many different identity systems are in use today, with still more being invented. As a result, the current state of digital identity on the Internet is an inconsistent patchwork of ad hoc solutions that burdens people with different user experiences at every website, renders the system as a whole fragile, and constrains the fuller realization of the promise of e-commerce.

The Internet’s Problems Are Often Identity Problems

Many of the problems facing the Internet today stem from the lack of a widely deployed, easily understood, secure identity solution.

A comparison between the bricks-and-mortar world and the online world is illustrative: In the bricks-and-mortar world, you can tell when you are at a branch of your bank. It would be very difficult to set up a fake bank branch and convince people to do transactions there. But in today’s online world, it is trivial to set up a fake banking site (or e-commerce site ...) and convince a significant portion of the population that it’s the real thing. This is an enormous identity problem. Websites currently do not have reliable ways of identifying themselves to people, thus enabling impostors to flourish. What is needed is reliable site-to-user authentication, which aims to make it as difficult to produce counterfeit services in the online world as it is to produce them in the physical world.

Conversely, problems identifying users to sites also abound. Username/password authentication is the prevailing paradigm, but its weaknesses are all too evident on today’s Internet. Password re-use, insecure passwords, and poor password management practices open a world of attacks, in and of themselves. Combine that with the password theft attacks enabled by counterfeit websites, and with man-in-the-middle attacks, and today’s Internet is an attacker’s paradise.

The consequences of these problems are severe and growing. The number of “phishing” attacks and sites has skyrocketed. There are reports that online banking activity is declining. Recent regulatory guidance on authentication in online banking reports that “Account fraud and identity theft are frequently the result of single-factor (e.g., ID/password) authentication exploitation.” [FFIEC 05] Consumer trust of the Internet is low and ever dropping [NCL 06] Clearly, the status quo is no longer a viable option.

What Is Needed: an Identity Metasystem

Given that universal adoption of a single digital identity system or technology is unlikely to occur, a successful and widely deployed identity solution for the Internet requires a different approach – one with the capability to connect existing and future identity systems into an identity metasystem. A metasystem, or system of systems, would leverage the strengths of its constituent identity systems, provide interoperability between them, and enable the creation of a consistent and
straightforward user interface to all of them. The resulting improvements in cyberspace would benefit everyone, ultimately making the Internet a safer place with the potential to boost e-commerce, combat phishing, and solve other digital identity challenges.

An identity metasystem could make it easier for users to stay safe and in control when accessing resources on the Internet. It could allow users to select from among a portfolio of their digital identities and use them for Internet services of their choice, where they are accepted. A metasystem could enable identities provided by one identity system technology to be used within systems based on different technologies, provided that an intermediary exists that understands both technologies and is capable and trusted to do the needed translations.

It is important to note that the role of an identity metasystem is not to compete with or replace the identity systems that it connects. Rather, a metasystem should rely on the individual systems in play to do its work!

**Architecture of a Proposed Solution**

By definition, in order for a digital identity solution to be successful, it needs to be understood in all the contexts when you may wish to use it to identify yourself. Identity systems are all about identifying yourself (and your things) in environments that are not yours. For this to be possible, both your systems and the systems that are not yours – those where you need to digitally identify yourself – must be able to speak the same digital identity protocols, even if they are running different software on different platforms.

Such a solution, in the form of an identity metasystem, has already been proposed, and some implementations are well underway. The identity metasystem is based upon an underlying set of principles called the “Laws of Identity.” The Laws are intended to codify a set of fundamental principles to which a universally adopted, sustainable identity architecture must conform. The Laws were proposed, debated, and refined through a long-running, open, and continuing dialogue on the Internet by the major players in the identity field. Taken together, the Laws are key to defining the overall architecture of the identity metasystem.

Because these Laws were developed through an open consensus process among experts and stakeholders, they reflect a remarkable convergence of interests, and are non-proprietary in nature. As a result, they have been endorsed and adopted by a long and growing list of industry organizations, associations, and technology developers.

By allowing different identity systems to work together in concert, with a single user experience, and a unified programming paradigm, the metasystem shields
users and developers from concerns about the evolution and market dominance of specific underlying systems, thereby reducing everyone’s risk and increasing the speed with which the technology can evolve.

It is our sincere belief that the 7 Laws of Identity and the identity metasystem they describe represent significant contributions to improving security and privacy in the online world and, as such, are worthy of closer study, support, and broad adoption by the privacy community.

We are particularly struck by the parallels with the fair information practices (FIPs), which set forth universal principles that both establish and confer broad rights on individuals with respect to the collection, use, and disclosure of their personal information by others, and, at the same time, set out broad responsibilities for organizations in respect to their collection, use, and disclosure of personal information. The FIPs have served as the basis for privacy and data protection laws around the world, and yet are versatile enough to be used to guide the design, development and operation of information technologies and systems in a privacy-enhancing manner.

We are impressed with how the Laws of Identity seek to put users in control of their own identities, their personal information, and their online experiences. In the metasystem, users decide how much information they wish to disclose, to whom, and under what circumstances, thereby enabling them to better protect their privacy. Strong two-way authentication of identity providers and relying parties helps address phishing and other forms of fraud. Identities and accompanying personal information can be securely stored and managed in a variety of ways, including via the online identity provider service of the user’s choice, or on the user’s PC, or in other devices such as secure USB keychain storage devices, smart cards, PDAs, and mobile phones.

Further, the identity metasystem enables a predictable, uniform user experience across multiple identity systems. It extends to and integrates the human user, thereby helping to secure the machine-human channel.

Participants in the identity metasystem may include anyone or anything that uses, participates in, or relies upon identities in any way, including, but not limited to, existing identity systems, corporate identities, government identities, Liberty federations, operating systems, mobile devices, online services, and smart cards. Again, the possibilities are only limited by innovators’ imaginations.

An example of a universal identity system that did not conform with the Laws of Identity is illustrative.
.Net Passport

Until now, Microsoft’s best-known identity effort was almost certainly the Passport Network, best known to millions of Internet users as a “single sign-on” identity system that stored users’ personal information centrally.

The identity metasystem is different from the original version of Passport in several fundamental ways. The metasystem stores no personal information, leaving it up to individual identity providers to decide how and where to store that information. The identity metasystem is not an online identity provider for the Internet; indeed, it provides a means for all identity providers to co-exist with and compete with one another—all having equal standing within the metasystem. And while Microsoft charged companies to use the original version of Passport, no one will be charged to participate in the identity metasystem.

In fairness, the Passport system itself has evolved in response to these experiences. It no longer stores personal information other than username/password credentials. Passport is now an authentication system targeted at Microsoft sites and those of close partners—a role that is clearly in context, and one with which users and partners are more comfortable. Passport and MSN plan to implement support for the identity metasystem as an online identity provider for MSN and its partners. Passport users will receive improved security and ease of use, and MSN Online partners will be able to interoperate with Passport through the identity metasystem.

An example of one desktop application, currently in development, that does embody the 7 Laws of the identity metasystem is also illustrative.

Cardspace and Information Cards

Microsoft, among others, is building user software that conforms to the 7 Laws of the identity metasystem. The “Cardspace” identity selector is a Windows component that provides the consistent user experience required by the identity metasystem. It is specifically hardened against tampering and spoofing to protect the end user’s digital identities and maintain end-user control. Each digital identity managed in Cardspace (comparable to a virtual card holder) is represented by a visual “information card” in the user interface. The user selects identities represented by information cards to authenticate to participating services.
Many identity attacks succeed because the user was fooled by something presented on the screen, not because of insecure communication technologies. For example, phishing attacks occur not in the secured channel between web servers and browsers – a channel that might extend thousands of miles – but in the two or three feet between the browser and the human who uses it. The identity meta-system, therefore, seeks to empower users to make informed and reasonable identity decisions by enabling the use of a consistent, comprehensible, and self-explanatory user interface for making those choices.

As Figure 1 illustrates, users can be in control of their identity interactions (see Laws 1 & 2) by being able to choose which identities to use at which services, by knowing what information will be disclosed to those services if they use them, and by being informed how those services will use the information they disclose. To be in control, you must first be able to understand the choices you are presented with (see Laws 6 & 7). Unless users can be brought into the identity solution as informed, functioning components of the solution, able to consistently make good choices on their own behalf, the problem will not be solved.
Information cards have several key advantages over username/password credentials:

- **No weak, reused, lost, forgotten, or stolen credentials**: Because no password is typed in or sent, passwords cannot be stolen or forgotten.

- **Better site authentication; less phishing**: Because authentication can be based on unique keys generated for every information card/site pair, the keys known by one site are useless for authentication purposes at another, even for the same information card. This directly addresses the phishing and fake website problems.

- **Data minimization**: Because information cards can re-supply identity information or claim values (e.g., name, address, and e-mail address) to other sites with whom they are dealing, those sites don’t need to store this data between sessions. Retaining less data, or data minimization, means that sites have fewer vulnerabilities. (See Law 2.)

- **Consistent interface = better choices**: Programs like Cardspace implement a standard user interface for working with digital identities. Perhaps the most important part of this interface, the screen used to select an identity to present to a site, is shown in Figure 1 on the previous page.

There are many information card systems. It is worth noting that, by extending the “real-world” visual metaphors and cues of the wallet containing various cards and credentials, information card software such as that by Microsoft makes it possible for users to be in better control of their digital identities. We encourage interested readers to read the seminal white papers freely available at www.identityblog.com, which further explain and clarify the Laws of Identity and information cards in greater detail.

Let us now turn to the privacy features embedded in the identity metasystem.

**Privacy Analysis and Commentary on the 7 Laws of Identity**

In light of the preceding discussion and the identity challenges and opportunities that lie ahead, we carried out the following privacy analysis and commentary on the 7 Laws of Identity (and, by extension, on the identity metasystem that those laws collectively describe).

The following chart is the summary result of our efforts to “map” fair information practices to the Laws of Identity, in order to explicitly extract their privacy-protective features. The result is a commentary on the Laws that “teases-out” their privacy implications, for all to consider.

In brief, the privacy-embedded Laws of Identity, when implemented, offer individuals:
The 7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity

- easier and more direct user control over their personal information when online;
- enhanced user ability to minimize the amount of identifying data revealed online;
- enhanced user ability to minimize the linkage between different identities and actions;
- enhanced user ability to detect fraudulent messages and websites, thereby minimizing the incidence of phishing and pharming.

### Laws of Identity

<table>
<thead>
<tr>
<th>The 7 Laws of Identity</th>
<th>7 Privacy-Embedded Laws of Identity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Law #1:</strong> User Control and Consent</td>
<td><strong>Law #1:</strong> Personal Control and Consent</td>
</tr>
<tr>
<td>Technical identity systems must only reveal information identifying a user with the user’s consent.</td>
<td>Technical identity systems must only reveal information identifying a user with the user’s consent. Personal control is fundamental to privacy, as is freedom of choice. Consent is pivotal to both. Consent must be invoked in the collection, use, and disclosure of one’s personal information. Consent must be informed and uncoerced, and may be revoked at a later date.</td>
</tr>
<tr>
<td><strong>Law #2:</strong> Minimal Disclosure for a Constrained Use</td>
<td><strong>Law #2:</strong> Minimal Disclosure for Limited Use: Data Minimization</td>
</tr>
<tr>
<td>The identity metasystem must disclose the least identifying information possible, as this is the most stable, long-term solution.</td>
<td>The identity metasystem must disclose the least identifying information possible, as this is the most stable, long-term solution. It is also the most privacy-protective solution. The concept of placing limitations on the collection, use, and disclosure of personal information is at the heart of privacy protection. To achieve these objectives, one must first specify the purpose of the collection and then limit one’s use of the information to that purpose. These limitations also restrict disclosure to the primary purpose specified, avoiding disclosure for secondary uses. The concept of data minimization bears directly upon these issues, namely, minimizing the collection of personal information in the first instance, thus avoiding the possibility of subsequent misuse through unauthorized secondary uses.</td>
</tr>
<tr>
<td><strong>Law #3:</strong> Justifiable Parties</td>
<td><strong>Law #3:</strong> Justifiable Parties: “Need-to-Know” Access</td>
</tr>
<tr>
<td>Identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.</td>
<td>Identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship. This is consistent with placing limitations on the disclosure of personal information, and only allowing access on a “need-to-know” basis. Only those parties authorized to access the data, because they are justifiably required to do so, are granted access.</td>
</tr>
<tr>
<td>The 7 Laws of Identity</td>
<td>7 Privacy-Embedded Laws of Identity</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td><strong>Law #4: Directed Identity</strong></td>
<td><strong>Law #4: Directed Identity: Protection and Accountability</strong></td>
</tr>
<tr>
<td>A universal identity metasystem must support both “omnidirectional” identifiers for use by public entities and “unidirectional” identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.</td>
<td>A universal identity metasystem must be capable of supporting a range of identifiers with varying degrees of observability and privacy. Unidirectional identifiers are used by the user exclusively for the other party, and support an individual’s right to minimize data linkage across different sites. This is consistent with privacy principles that place limitations on the use and disclosure of one’s personal information. At the same time, users must also be able to make use of omnidirectional identifiers provided by public entities in order to confirm who they are dealing with online and thereby ensure that their personal information is being disclosed appropriately. To further promote openness and accountability in business practices, other types of identifiers may be necessary to allow for appropriate oversight through the creation of audit trails.</td>
</tr>
<tr>
<td><strong>Law #5: Pluralism of Operators and Technologies</strong></td>
<td><strong>Law #5: Pluralism of Operators and Technologies: Minimizing Surveillance</strong></td>
</tr>
<tr>
<td>A universal identity solution must utilize and enable the interoperation of multiple identity technologies run by multiple identity providers.</td>
<td>The interoperability of different identity technologies and their providers must be enabled by a universal identity metasystem. Both the interoperability and segregation of identity technologies may offer users more choices and control over the means of identification across different contexts. In turn, this may minimize unwanted tracking and profiling of personal information obtained through surveillance of visits across various sites.</td>
</tr>
<tr>
<td><strong>Law #6: Human Integration</strong></td>
<td><strong>Law #6: The Human Face: Understanding is Key</strong></td>
</tr>
<tr>
<td>The identity metasystem must define the human user to be a component of the distributed system, integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.</td>
<td>Users must figure prominently in any system, integrated through clear human-machine communications, offering strong protection against identity attacks. This will advance user control, but only if users truly understand. Thus, plain language in all communications used to interface with individuals is key to understanding. Trust is predicated on such understanding.</td>
</tr>
<tr>
<td><strong>Law #7: Consistent Experience across Contexts</strong></td>
<td><strong>Law #7: Consistent Experience across Contexts: Enhanced User Empowerment and Control</strong></td>
</tr>
<tr>
<td>The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.</td>
<td>The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies. We return full circle to the concept of individual empowerment and informed consent. Clear interfaces, controls and options that enhance an individual’s ability to exercise control across multiple contexts in a reliable, consistent manner will serve to enhance the principle of informed consent.</td>
</tr>
</tbody>
</table>
Conclusions

The Internet was built without a way to know who and what individuals are communicating with. This limits what people can do and exposes computer users to potential fraud. If nothing is done, the result will be rapidly proliferating episodes of theft and deception that will cumulatively erode public trust. That confidence is already eroding as a result of spam, phishing, pharming and identity theft, which leaves online consumers vulnerable to the misuse of their personal information and minimizes the future potential of e-commerce. The privacy-embedded 7 Laws of Identity support the global initiative to empower consumers to manage their own digital identities and personal information in a much more secure, verifiable and private manner.

Identity systems that are consistent with the privacy-embedded 7 Laws of Identity will help consumers verify the identity of legitimate organizations before they decide to continue with an online transaction. Consumers today are being spammed, phished, pharmed, hacked and otherwise defrauded out of their personal information in alarming numbers, in large part because there are few reliable ways for them to distinguish the “good guys” from the “bad.”

E-commerce providers are taking note of this trend because declining consumer confidence and trust are especially bad for business. The next generation of intelligent and interactive web services (Web 2.0) will require more, not fewer, verifiable identity credentials, and much greater mutual trust in order to succeed.

Just as the Internet emerged from connecting different proprietary networks, an “Identity Big Bang” is expected to happen once an open, non-proprietary and universal method to connect identity systems and ensure user privacy is developed, in accordance with universal privacy principles. Already, there is a long and growing list of companies and individuals that endorse the 7 Laws of Identity and are working toward developing identity systems that conform to them. Participants include e-commerce sites, financial institutions, governments, Internet service providers, mobile telephony operators, certificate authorities, and software vendors for a broad range of platforms.

Our efforts to describe the 7 privacy-embedded Laws of Identity are intended to inject privacy considerations into discussions involving identity – specifically, into the emerging technologies that will define an interoperable identity system. We hope that our commentary will stimulate broader discussion across the Internet blogosphere and among the “identerati.”

We also hope that software developers, the privacy community and public policymakers will consider the 7 privacy-embedded Laws of Identity closely, discuss them publicly, and take them to heart. Promoting privacy-enhanced identity solutions at a critical time in the development of the Internet and e-commerce will enable both privacy and identity to be more strongly protected.
APPENDIX A: Fair Information Practices

CSA Privacy Code

Principles in Summary

Ten interrelated principles form the basis of the CSA Model Code for the Protection of Personal Information. Each principle must be read in conjunction with the accompanying commentary.

1. **Accountability:** An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization’s compliance with the following principles.

2. **Identifying Purposes:** The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

3. **Consent:** The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

4. **Limiting Collection:** The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. **Limiting Use, Disclosure, and Retention:** Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

6. **Accuracy:** Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

7. **Safeguards:** Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. **Openness:** An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

9. **Individual Access:** Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. **Challenging Compliance:** An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization’s compliance.

Source: www.csa.ca/standards/privacy
APPENDIX B: Information Sources and Other Useful Reading Materials

The Case for Privacy-Embedded Laws of Identity in the Digital Age

Identity Theft Revisited: Security Is Not Enough

www.ipc.on.ca

Kim Cameron’s Identity Weblog

www.identityblog.com

The LAWS OF IDENTITY
An introduction to Digital Identity – the missing layer of the Internet

www.identityblog.com/?page_id=354

The IDENTITY METASYSTEM
A proposal for building an identity layer for the Internet

www.identityblog.com/?page_id=355

Identity Management Research & Development Projects

• InfoCard / CardSpace: www.identityblog.com/wp-content/resources/design_rationale.pdf
• Open Source identity Selector (OSIS) project: http://osis.netmesh.org
• Shibboleth: http://shibboleth.internet2.edu/about.html
• Yadis: http://yadis.org & www.openidenabled.com
• OpenID: www.openid.net & www.openidenabled.com
• Private Credentials: www.credentica.com
• Liberty Alliance Project: www.projectliberty.org

Identity Management Research

• EU Privacy and Identity Management for Europe (PRIME): www.prime-project.eu

Select Analyst and Media Information Sources

Privacy in the Clouds:
A White Paper on Privacy and Digital Identity

May 2008
Privacy in the Clouds:  
A White Paper on Privacy and Digital Identity

Introduction

Informational self-determination refers to the ability of individuals to exercise personal control over the collection, use and disclosure of their personal information by others. It forms the basis of modern privacy laws and practices around the world.

All organizations that collect and use personal data must accommodate the legitimate interests of individuals. Organizations can do this, for example, by being open and accountable about their information management practices, by seeking informed consent, and by providing individuals with access and redress mechanisms. At stake is not only privacy, but also the confidence and trust of millions of individuals, consumers, and citizens in today’s information society.

At the Office of the Information and Privacy Commissioner of Ontario (IPC), we have long advocated a strong role for individuals in managing their personal information, not just by exercising their privacy rights under Ontario law, but also by becoming better informed and using privacy-enhancing technologies (PETs). PETs can minimize the disclosure and (mis)use of personally identifiable information (PII), and help secure data from unauthorized use by others.

Informational self-determination has become a challenging concept to promote and protect in a world of unlimited information passing from individuals to organizations, and from organizations to each other, often described as “Web 2.0.” As a result of widespread developments in information and communications technologies (ICTs), we are collectively creating, storing and communicating information at nearly exponential rates of growth. A large majority of this data is personally identifiable, and much of it is under the control of third parties. Practical obscurity – the basis for privacy norms throughout history – is fast disappearing.

Our digital footprints and shadows are being gathered together, bit by bit, megabyte by megabyte, terabyte by terabyte, into personas and profiles and avatars – virtual representations of us, in a hundred thousand simultaneous locations. These are used to provide us with extraordinary new services, new conveniences, new efficiencies, and benefits undreamt of by our parents and grandparents. At the same time, novel risks and threats are emerging from this digital cornucopia. Identity fraud and theft are the diseases of the Information Age, along with new forms of discrimination and social engineering made possible by the surfeit of data.
Privacy by Design

Personal information, be it biographical, biological, genealogical, historical, transactional, locational, relational, computational, vocational, or reputational, is the stuff that makes up our modern identity. It must be managed responsibly. When it is not, accountability is undermined and confidence in our evolving information society is eroded.

It may very well be that our fundamental ideas about identity and privacy, the strategies that we have collectively pursued, and the technologies that we have adopted, must change and adapt in a rapidly evolving world of connectivity, networking, participation, sharing, and collaboration.

What will privacy mean, and how will privacy survive and hopefully, thrive, as a viable human right, operational value, and critical enabling trust factor in a world where the individual is less and less directly present in the midst of data-rich transactions?

How will individuals exercise control over their personal data when that data is stored and processed in the Cloud\(^1\) – that is, everywhere except on their own personal computing devices?

Profound and dramatic transformations and upheavals are on the way. How will privacy fare?

---

1 In telecommunications, a “Cloud” is the unpredictable part of any network through which data passes between two end points. For the purposes of this paper, the term is used to refer generally to any computer, network or system through which personal information is transmitted, processed and stored, and over which individuals have little direct knowledge, involvement, or control.
The 21st Century Privacy Challenge

The Internet has entered into a new phase. Thanks to more reliable, affordable and ubiquitous broadband access, the Internet is no longer just a communications network. It is becoming a platform for computing – a vast, interconnected, virtual supercomputer. Many different terms have been used to describe this trend: Web 2.0, Software as a Service (SaaS), Web Services, “Cloud computing,” and the Grid. Each of these terms describes part of a fundamental shift in how data are managed and processed. Rather than running software on a desktop computer or server, Internet users are now able to use the “Cloud” – a networked collection of servers, storage systems, and devices – to combine software, data, and computing power scattered in multiple locations across the network.

The importance of this shift cannot be overstated. To quote Nicholas G. Carr, it “will overturn strategic and operating assumptions, alter industrial economics, upset markets and pose daunting challenges to every user and vendor. The history of the commercial application of information technology has been characterized by astounding leaps, but nothing that has come before – not even the introduction of the personal computer or the opening of the Internet – will match the upheaval that lies just over the horizon.”

The new digital ecosystem will also present complex security and privacy challenges. Fundamentally, it will need to provide flexible, user-friendly ways to authenticate users. Without better management of digital identities, we will not only continue to struggle with existing problems such as identity theft, spam, malware, and cyber-fraud, we will be unable to assure individual users that they can safely migrate their critical data and applications from their own computers onto the Web. The opportunity presented by technological development will be lost.

Evolution of Consumer Computing

From a user’s perspective, the evolution of consumer computing can be divided into three phases:

1. **The stand-alone personal computer**, in which the user’s operating system, word processing system, database software and data are stored on a single, easily protected machine. Examples: word processing, spreadsheets on a stand-alone server.

2. **The Web**, in which most of the software users need is still on their own PC, but more and more of the data they need is found on the Internet. Example: using a Web browser to read a Web page.

---

3 The **Cloud,** in which users rely heavily on data and software that reside on the Internet. Examples: using Amazon’s Simple Storage Service (S3) and Elastic Computing Cloud (EC2) to store unlimited photos on Smugmug, an online photo service; using Google Apps for word processing; virtual worlds such as Second Life that enable users to build 3-D environments combining Web pages and Web applications (e.g., feeding a Webcast into a virtual theatre); grid computing.

**The Power and Promise of Cloud Computing**

Most of the work we do with computers is still conducted using phase 1 or 2 tools, but more and more people – especially younger generations – are starting to take advantage of the power of the Cloud. The Cloud offers them so much:

1 **Limitless flexibility:** With access to millions of different pieces of software and databases, and the ability to combine them into customized services, users are better able to find the answers they need, share their ideas, and enjoy online games, video, and virtual worlds;

2 **Better reliability and security:** Users no longer have to worry about their hard drives crashing or their laptops being stolen;

3 **Enhanced collaboration:** By enabling online sharing of information and applications, the Cloud offers users new ways of working and playing together;

4 **Portability:** Users can access their data and tools wherever they can connect to the Internet;

5 **Simpler devices:** With data and the software being stored in the Cloud, users don’t need a powerful computer. They can interface using a cellphone, a PDA, a personal video recorder, an online game console, their cars, or even sensors built into their clothing.

We can only enjoy the full benefits of Cloud computing if we can address the very real privacy and security concerns that come along with storing sensitive personal information in databases and software scattered around the Internet.

Digital identity is a fundamental challenge. In phase 1 of consumer computing, users’ privacy and security was largely assured by restricting physical access to the stand-alone computing devices and storage media. Identity needs were fairly minimal, consisting largely of a small handful of usernames and passwords for local systems and file access.

---

In phase 2 of consumer computing, users usually have to establish their identity each time they use a new Internet-based application, usually by filling out an online form and providing sensitive personal information (e.g., name, home address, credit card number, phone number, etc.). This leaves a trail of personal information that, if not properly protected, may be exploited and abused.

**Identity Service Requirements in the Cloud**

Cloud computing and the exciting tools it makes possible (like virtual worlds, grid computing, and shared archives), require identity services that:

1. are independent of devices;
2. enable a single sign-on to thousands of different online services;
3. allow pseudonyms and multiple discrete (but valid) identities to protect user privacy;
4. are interoperable, based on open standards, and available in open source software (in order to maximize user choice);
5. enable federated identity management; and
6. are transparent and auditable.

This paper explores what will be possible if proper digital identity services are deployed and the full power of Cloud computing is realized. A number of scenarios are described:

1. an identity service that enables individuals to easily manage their own online identities and to effortlessly participate in online collaboration activities without repeated sign ons;
2. an identity tool that gives users of an online dating service better privacy than is available from today’s sites;
3. a payment system using cellphones or RFID chips that has privacy built in;
4. an infrastructure for electronic health records; and
5. an identity service for virtual worlds such as Second Life.

**The Digital Identity Situation Today**

Almost all online activities, such as sending e-mails, filing tax declarations, managing bank accounts, buying goods, playing games, connecting to a company Intranet, and meeting people in a virtual world, require identity information to be given from one party to another. Today, most users have to establish their identity each time they use a new application, usually by filling out an online form and providing sensitive personal information (e.g., name, address, credit card number, phone number, etc.).
A typical Internet user in Canada has provided some type of personal information to dozens of different websites. If you count cookies and IP addresses as personal information, then Internet users have left behind personally identifiable information everywhere they've been. They have left “digital bread crumbs” throughout cyberspace – and they have little idea how that data might be used, or how well it is protected.

The Digital Identity Needs of Tomorrow
What is needed is flexible and user-centric identity management. Flexible, because it needs to support the multitude of identity mechanisms and protocols that exist and are still emerging, and the different types of platforms, applications and service-oriented architectural patterns in use; user-centric because end-users are at the core of identity management. Users must be empowered to execute effective controls over their personal information.

In the future, users will not have to re-enter personal data each time that they go to a new website. Instead, by using an identity service (or two or more different ones), they will have control over who has their personal data and how it is used – minimizing the risk of identity theft and fraud. Their identity and reputation will be transferable. If they establish a good reputation, for example, at an auction site, they will be able to use that fact on other sites as well. One result of this would be greater choice of online services, since users would not be locked into one service or vendor.
A truly flexible identity management system would not be limited to laptop and desktop computers; it would work on cellphones, personal digital assistants, smart cards, sensors, consumer electronics like video recorders and online game consoles – any way that a user might touch the Internet. This approach to digital identity will unleash the full potential of the Cloud, enabling users to seamlessly tap into and combine a wide range of online services.

Case studies
1 The “Live Web”
The Internet has become a vastly more connected and interactive place for millions of people to spend their time. By any measurement index – growth in blogs, collaborative wikis, mash-ups, and online social networks – the phenomenon of the “participatory Web” is transforming our lives with virtually limitless opportunities to become engaged, customize experiences, and find our own individual public voices.

This proliferation of online activity requires sound identity management. With the increased use of the Internet to conduct business and the rise of new types of online interactions, such as social networking and user-generated content, innovative kinds of digital identifier technologies are necessary to sustain the “open Web.” Online users need to securely manage their multiple accounts and passwords across multiple domains, without fear of surveillance and profiling.

In order to facilitate this, OpenID, developed by an open community, is free “user-centric” digital identity technology that simplifies the online user experience by reducing the complexity of managing dozens, even hundreds of user names and passwords across Internet sites, and providing greater control over the personal information users are required to share with websites when they sign in.
OpenID enables individuals to convert one of their already existing digital identifiers – such as their personal blog’s URL – into an OpenID account, which can then be used as a login at any website supporting OpenID.

Today, more than 10,000 websites support OpenID logins, and an estimated 350 million OpenID-enabled URLs currently exist.

For online businesses, these efforts can lower password and account management costs, help reduce the overall risks of security breaches by limiting the amount of customer personal information they need to store and protect, and increase both new and return user traffic by lowering the barriers to website entry and re-entry.

2 Online Dating
An online dating service matches people together based on their personal interests and preferences using some sophisticated matching algorithms. The matching algorithm needs a good deal of personal data in order to work, and therefore users of those dating services need strong assurances that their information will be treated with respect and used only for the intended and agreed-upon purposes.

Even if a user agrees to receive marketing e-mails from third parties, for example, they may nonetheless want to be certain that their personal details will not be given to those third parties. For instance, someone who is overweight may not wish to receive marketing e-mails from makers of “full-size” clothing.

To protect privacy, dating services could allow their clients to use pseudonyms rather than their real names. The dating service has no business need to know the real identities of their customers, other than their need to get paid, which could be done through a pre-paid or cash-like service.

Today, customers of dating services can claim almost any attribute, and nothing prevents “devils” from impersonating “angels.” With better digital identity management, the dating service would be able to accept third-party certified attributes, without customers running the risk that the certificates would reveal their real names to the service. For instance, a certified date of birth might give a higher rank in the matchmaking algorithms than an uncertified one. A certificate that a customer is not listed in a certain blacklist might be mandatory for certain dating services. Such an approach would reduce the risk of misrepresentation and increase the level of trust, without impacting on privacy.

When customers finally get introduced to each other, they could potentially use the identity management mechanisms to establish increasing trust in each other in a multi-round “game,” checking each others’ attributes in the safety and privacy of their homes. They could even ask each other questions like “are you younger than me?” and so on, without having to reveal their actual birthdays, but rather, just a birth year or range.
3 Cellphone Payments and Location-Dependent Services
One very promising development in the cellphone industry is the deployment of cellphones as “digital wallets” that can be used to transfer and store money, pay parking meters and vending machines, and eventually act as a kind of a credit card. Privacy concerns, however, are a major barrier to the adoption of this technology.

Many consumers are already uncomfortable knowing that credit card companies can compile a detailed record of their spending behaviour. With electronic wallets, it is conceivable that your cellular phone provider would not only know when, where, and how you were spending your money, but by tracking others’ electronic wallets, they could know who you were with when you spent it (at a restaurant or a hotel, for instance).

User-centric identity management would allow the users of an “electronic wallet” to use a digital identity service to authenticate themselves, without revealing their actual identity to either vendors or network providers.

4 Health-Care Records
Some of the most sensitive personal information about us is associated with the medical services and medications we use. Yet today, that personal information is scattered in dozens of different locations, including doctors’ offices, pharmacies, insurance companies, and our places of employment.

One of the biggest barriers to the widespread adoption of electronic health records has been the concern of patients that their data in such records will be misused or stolen. We have already seen too many examples of sensitive medical or drug data being used for inappropriate or unauthorized purposes.

User-centric identity management could ensure that someone’s real name (and the personal data that could be used to infer who they are) would be protected and kept separate from the details of their medical records, insurance claims, and drug prescriptions. It would also enable a patient to use an online portal with a federated identity system to quickly and safely access all their medical information, whether it be stored at their doctor’s office, their pharmacy, or their insurance company. Perhaps most importantly, there would be the ability to audit these records and determine where personal data is stored, how it is protected, and who has had access to it.

5 Identity and Trust in Virtual Worlds
Over the last year, there have been a number of press reports on virtual worlds such as Second Life and There.com, and online games such as World of Warcraft. Millions of people are spending hours a week in these immersive, three-dimensional online environments, finding new ways to collaborate, play games, and share information. Virtual economies are also developing as inhabitants of these virtual worlds buy and sell virtual goods and services, exchanging millions of real dollars every year.
Unfortunately, there are currently no effective means for managing identity and security in most virtual worlds. As a result, it is difficult to prevent disruptive behaviour or inappropriate postings by anonymous users who may appear and quickly disappear. This lack of security and trust is slowing the development of serious business applications in virtual worlds.

User-centric identity management could provide an effective way to build trusted communities in the virtual world. For instance, parents could rest assured that when their children went online to play in a virtual world for kids, every other person there had been properly authenticated and was really a “child.”

One of the most exciting reasons for the phenomenal growth of virtual worlds like Second Life is that they allow users to create new services and to “plug in” applications from elsewhere on the Web. With user-centric identity management, you could establish your identity once and then be able to use the full range of services in a virtual world. And an identity established in Second Life could then be transferable into another virtual world. But you would not have to share your personal information in any other “world” unless you chose to.

**Creating a User-Centric Identity Management Infrastructure**

The goal of a flexible, user-centric identity management infrastructure must be to allow the user to quickly determine what information will be revealed to which parties and for what purposes, how trustworthy those parties are and how they will handle the information, and what the consequences of sharing their information will be. In other words, these tools should enable users to give informed consent. The default should be minimal disclosure, for a defined purpose. Any secondary or additional use should be optional after enrolment.

Companies need to understand that identity management is not only a business process, but also a user activity. Users must be given adequate tools to manage the personal information on all of their devices. This means that the identity infrastructure must account for many devices, from desktop PCs to mobile phones. The infrastructure must allow for a unified user experience over all devices.

It also means that the system must be driven throughout by a clear framework of agreed-upon rules. This includes policies describing to users what information is requested and why (similar to a machine-readable and improved version of today’s privacy policies). It must also include a “sticky” policy that travels with the information throughout its lifetime and ensures that it is only used in accordance with the policy. The last step will of course require mechanisms to enforce these sticky policies in ways that can be verified and audited.
There are already a number of identity management systems in place on a wide variety of platforms. These need to be supported, at least in the short term, by the identity management infrastructure. The infrastructure must support cross-system interaction as well as interoperation and delegation between them. This is only possible if the infrastructure and the individual systems are based on open standards, available on all platforms. For a successful user-centric identity management infrastructure to emerge, it is crucial that its development be driven by a wide and open community, spanning the different geographies and cultures, and that open source implementations of all of its infrastructural components be made available.

Identity information is almost always personally identifiable information, which is governed by special privacy regulations in many parts of the world. Further, an improper use of identity information may lead to identity theft and other breaches of security. Thus, identity information requires special protection. This includes, among other things, the ability to carry and enforce sticky policies, encrypt data, and minimize the amount of identity information used by various applications. Actual identity management systems will support a wide variety of privacy and various security properties, ranging from low-security password-based one-factor authentication to high-end, attribute-based systems deploying state-of-the-art privacy-enhancing certificates (for example, IBM’s Identity Mixer technology, or Microsoft’s U-Prove technology). While the infrastructure needs to support all of these systems, users should understand the implications of using one system over the other.

At the end of the day, applications need to be able to make use of the infrastructure. This requires that applications be presented with a unified view and interfaced to this infrastructure across different platforms and devices. These interfaces should be independent of the actual protocols and mechanisms that are used to convey the identity information underneath. Therefore, we are proposing a single architecture that pulls the different pieces together and unifies them.

By supporting a plethora of identity systems, this architecture will allow for the migration of applications from legacy systems to the user-centric ones that will emerge and prevail. To enable such migration, as well as building applications from scratch, adequate tools and sample applications will need to be provided.

**Open Standards and Community-Driven Interoperability**

The Internet was founded on open standards and collaboration. Open standards facilitate a reliable base for customers, applications, and enterprises. As such, they form an important foundation for the growth of the future Web and nurture the development of an open identity management ecosystem for the whole industry.

To enable the federation and interoperability of the different existing and emerging identity management systems, the underlying standards and specifications need to be complete, freely accessible, and, most important, driven by the community.
To have user-centric identity management widely adopted, the standards and tools provided need to be free from IP infringements. This will allow for a supporting ecosystem to grow and be maintained, not only by multinational companies but also by open-source initiatives and start-ups. So it is essential that standards be published widely and on a timely basis, and that they be stable and enduring.

Open standards are required to support the plethora of environments and application scenarios in which identity management plays a critical role and to enable inter-operation of these environments. In particular, communication formats and policy specifications act as medium for the interconnection of client and server-sides. This medium can only form the basis for a lively and value-generating ecosystem if it is based on the principles of truly open standards.

The standards – rather than the particular implementations by single vendors or consortia – must form the basis of regular interoperability tests. Moreover, they need to be controlled by an impartial, credible standards organization that governs the freely available open standards for the benefit of the entire community.

Protecting Privacy

The Internet was designed to connect and authenticate devices with logical and physical address spaces. User-centric identity services can provide the same ubiquitous connectivity for individuals. An identity today is no longer a single number assigned to an individual but rather comprises a set of attributes including address, birth date, degrees held, and personal preferences. Such personal information requires special protection, not only to prevent fraud and identity theft, but also to comply with privacy laws.

Most existing laws have their roots in the Organisation for Economic Co-operation and Development’s (OECD) privacy guidelines. These stipulate, for example, that only the personal information needed for a stated purpose should be collected, that the collection should be openly communicated, that the user must give informed consent to the collection and use, and that the personal information must be properly safeguarded.4

Identity management systems can support compliance with privacy laws through the use of privacy policies, enforcement mechanisms, and technologies that allow applications to use only the amount of personal information that is strictly necessary to the application. Policies that outline what information is being sought and the reasons why, enable users to give informed consent. These policies will also govern access controls, and should travel with the data for the course of their lifetime.

4 In 2006, the IPC led an international group of privacy and data protection commissioners to develop a set of fair information practices that harmonized the various privacy codes and practices currently in use around the world. The result – the Global Privacy Standard – can be found at: www.ipc.on.ca/images/Resources/up-gps.pdf
Already there exist privacy-enhancing technologies that allow a user to give an authentication token containing only an encrypted form of the user’s identity to a service provider. This allows the user to appear anonymously to the service provider while still making it possible to reveal true identity in the event of an investigation by a designated authority. Strong restrictions and conditions would be placed on an authority’s ability to revoke a user’s anonymity.

**Diversity for a Lively Ecosystem**
There is currently a great deal of diversity in identity management systems, along with a multitude of open standards that support identity federation and user-centricity for these systems. The most prominent examples are probably SAML, OpenID, and the WS-Federation specifications. Each of these has pros and cons, and contributes in different ways to the emerging ecosystem.

While these efforts will likely converge over time, the present diversity may be inspiring and potentially drive positive new developments in identity management. New models and protocols are being developed and deployed. Further methods will evolve, and there will be niches and application scenarios in which some specific solutions will surpass mainstream standards and protocols.

Investments have already been made in deploying system-based identity management products like Liberty Alliance or WS-Federation. The emerging ecosystem needs to support the existing diversity while allowing new solutions and concepts to be applied, as other solutions fade out gracefully.

**Diversity for User Devices**
While user-centricity is mostly discussed with PCs in mind, users will want to use a number of other devices, such as mobile phones or electronic identity cards, to take part in the information society. They may even wish to use devices that they do not personally own.

This diversity of clients requires that the identity management system be flexible, offering users a maximum number of choices as well as the best security and privacy protection possible.

**Collaboration of Users**
The boundaries of corporations are becoming less defined, with virtual companies emerging. Further, user contributions and collaboration are becoming increasingly central to many emerging applications. These scenarios have in common the need to deal with users who have not been physically identified, but are judged by their reputation or other attributes (such as area of expertise, education, age, etc.), as attested to by third parties.

The emerging identity information infrastructure must support such a collaborative environment – allowing for decentralized and federated trust models based on limited identity information (e.g., the current user is a medical expert).
Technology Building Blocks

These different scenarios will require a number of different technology building blocks, including:

- **Open source and proprietary identity software based on open standards**, which can be easily incorporated into the full range of online services and devices (similar to the open source software that is at the core of the Internet and the Web today).

- **Federated identity**, so that once users have authenticated themselves with one service or institution, their identity credentials will be recognized elsewhere. Brokering of security and authentication will eliminate the need to use a different stand-alone log-on process for each application or online service.

- **Multiple and partial identities**, so that users can access online services, explore virtual worlds, and collaborate with others without necessarily revealing their name and true identity to everyone. Different pseudonyms should support differing ranges of identification and authentication strengths.

- **Data-centred policies**, that are generated when a user provides personal or sensitive information, that travels with that information throughout its lifetime to ensure that the information is used only in accordance with the policy, e.g., for the purposes for which it was intended and which the user had consented to.

- **Audit tools**, so that users can easily determine how their data is stored, protected, and used, and determine if the policies have been properly enforced.

A Call to Action

It will not be possible to realize the full potential of the next generation of the Internet and Cloud Computing without developing better ways of establishing digital identity and protecting privacy.

Fortunately, progress is being made in developing and deploying the technological tools needed. But barriers remain. Different segments of the “IT ecosystem” can take steps to overcome them:

- Corporate and individual users can explore the evolving identity systems and demand that they have privacy protection built in, as well as implementing open standards so that different systems will be truly interoperable;

- Standards bodies can continue to develop and promote the fundamental standards needed for identity systems, data-centred policies, and privacy-enhancing technologies;
Software vendors and website developers can embrace privacy-enhancing technologies, open standards, open identity management systems, and true interoperability;

Governments, through their procurement decisions, can support the development of open identity management systems that are designed to meet user needs for privacy, interoperability, and flexibility.

The brave new world of Cloud Computing offers many benefits provided that the privacy and security risks are recognized and effectively minimized.

User-centric private identity management in the Cloud is possible, even when users are no longer in direct possession of their personal data, or no longer in direct contact with the organization(s) that do possess it.

This paper has outlined some technical building blocks and challenges that will become essential elements of a privacy-friendly Web 2.0 world. To be sure, laws, standards, education, awareness, and market forces will also be needed to support this vision.

Widespread and enduring user trust depends on realizing this vision. But how can we collectively assure confidence and trust in the privacy of our personally identifiable information when our identity data is held by others and we are not directly involved in data transactions in Cloud?

Four fundamental technological approaches present themselves:

1 Trust the data to behave:
   New privacy-enhancing information technologies make it possible to attach individual privacy rights, conditions and preferences directly to their own identity data, similar to digital rights management technologies for intellectual property.

2 Trust the personal device to interface and act on our behalf:
   The many technologies that travel with us are growing in storage, computing, and communications sophistication. Cellphones, PDAs, smart cards and other tokens under our physical control are becoming our de facto digital wallets, interacting with the “grid” and serving as brokers and proxies for our identity-based transactions in the digital world. These devices need to be trustworthy, fully user-configurable, user-transparent and easy to use.

3 Trust the intelligent software agents to behave:
   Whether operating on our “always-on” Internet devices, or housed somewhere in the Cloud, intelligent software agents can automatically and continuously scan, negotiate, do our bidding, reveal identity information, and act on our behalf in a Web 2.0 world. Some examples may include delegated identity tools, “reachability” software, and “privacy bots.”
4 Trust intermediary identity providers to behave:

Inevitably, we must also have sufficient trust in those organizations that would supply and accept our identity credentials and our personally identifiable information. In a federated identity world, these trusted actors will increasingly act on our behalf, disclosing our identity data for the purposes we define in advance, and under specific conditions. They must find credible technological mechanisms for assuring us that they are behaving in an open and accountable manner, and that our privacy is, in fact, being protected. Possible technologies might include automated audit and enforcement tools that can also convey up-to-the-minute privacy and security status reports to users, regulators and other trusted third parties.

The Office of the Information and Privacy Commissioner of Ontario remains committed to seeking privacy-enhanced technology solutions to the growing digital identity needs of today and tomorrow.

To this end, we hope to encourage greater understanding, participation and dialogue among all stakeholders in the identity world of the essential privacy issues at play, and of the solutions possible.

We call upon all stakeholders and technology developers, in particular, to develop trusted mechanisms for assuring widespread and enduring user confidence in the privacy and security of their identity data in the Web 2.0 world of the future.

Let the dialogue begin!
Privacy and the Open Networked Enterprise

Foreword

This white paper represents a joint effort between the Information and Privacy Commissioner of Ontario (IPC) and the New Paradigm Learning Corporation (NPLC). In 2004, the NPLC launched the Information Technology and Competitive Advantage program to examine the impact of information technology on business strategies in the 21st century. This in turn led to the conceptualization of the “Open Networked Enterprise,” or the ONE. This paper is an analysis of information privacy and security issues relating to both companies and consumers.

A number of high-profile privacy breaches have drawn to the attention of consumers how important it is to be aware of who is in possession of their information and how it is being used. Consumers are getting much smarter, no longer blindly accepting that companies need to know everything about them in order to “serve them better” or get better products. Many businesses are now beginning to encounter consumers who want to have a say in what information they will give out and who is permitted to use it. Privacy is no longer just a compliance issue – it has become a business issue. The successful companies of the future will be those who accept the present-day fact that “privacy is good for business,” and ultimately leads to a competitive advantage.

Ann Cavoukian, Ph.D.
Commissioner
June 2005

The Idea in Brief

Companies that take advantage of an Open Networked Enterprise (ONE) have the ability to become increasingly inter-networked, and to share more and different kinds of information than ever before. But while this network allows for greater transparency of information, it also raises the central issue of privacy. By necessity, within an ONE corporate boundaries blur: in order to facilitate effective collaboration, the ONE compiles highly granular data from disparate sources (i.e., multiple stakeholders) to create a more holistic business intelligence. However, as active ONES become increasingly global, this information may come from jurisdictions with looser privacy laws than the home company and, problematically, may overlap with personal information.

At stake in this march toward global transparency is the value of information itself, especially personally identifiable information (PII). The lifeblood of the 21st century
economy, information must increasingly be viewed as both an asset and a liability that requires responsible management practices. A company adopting an ONE model is confronted with fundamental questions relating to its treatment of information:

1. With whom will it share its PII?
2. How will it manage that data internally?
3. How should it involve customers in managing their own PII?
4. What personal data will and should it receive from others?
5. Where should it set the limits of PII collection by new technologies?

New information technologies inevitably affect levels of personal privacy. History has taught us that excesses and abuses of personal information tend to provoke backlashes in the form of counter-reactive behaviour by consumers and legislative/regulatory bodies. Most, if not all, of the privacy issues described in this paper are currently subjects of heightened public awareness and controversy, and it is public awareness and controversy that lead to regulation and legislation.

For these and many other good reasons, a company’s ONE model is well advised to meet the highest standards of responsible information management. By treating personal information responsibly, companies can harness the capabilities of a new breed of consumers, privacy hawks, who have strong views about personal information and privacy. Smart firms will build appropriate and effective privacy policies and practices into their systems. In doing so, these firms can avoid potential disasters and create the conditions for trust, loyalty, long-term relationships and economic advantage. Privacy is no longer a compliance issue; it is a business issue. It must be a business imperative.

The context: privacy and technology

The rise in modern communications has brought the issue of privacy to the forefront of public consciousness. Indeed, the modern concept of privacy emerged in reaction to information and communications technologies in the late 1800s that suddenly make it possible to effectively capture, store and disseminate information on a mass scale never before contemplated. With the development of the photograph, telegraph and mass printing methods the world began to shrink. The emergence of the “yellow press” in the early part of the 20th century triggered the earliest definition of privacy as personal freedom from unwanted intrusions, or “the right to be let alone.” From constitutional protection against search and seizure to restrictions upon free speech, to the implementation of slander and tort laws, common law in the 20th century tended to recognize and respond to privacy threats principally in terms of intrusion upon an individual’s personal space and private conversations, as well as upon his or her good name and reputation.
The appearance of mainframe computers, centralized electronic databases and
computerized records in the 1960s and 1970s triggered the next wave of privacy
protections. The large-scale collection by governments of secret, centralized
dossiers on citizens and the frequent misuse of that information led to the devel-
opment of laws to restrict governments’ abilities to compile and use such records.
At the same time, however, freedom of information laws were also enacted to pro-
mote greater openness and transparency for the sharing of new classes of infor-
mation with multiple stakeholders and to enhance individuals’ rights of access to
personal information in those databases.

In response to the misuse of large-scale computerized databases by private or-
ganizations in the financial, credit and medical sectors, similar “sunshine” laws
were also put in place to protect individuals and their highly personal information,
such as credit or health records. Fundamental “privacy” principles came into wide-
spread currency, such as those set out by the U.S. Family Educational Rights and
Privacy Act of 1974:1

- **Collection Limitation:** There must be no personal data record keeping sys-
tems whose very existence is secret.

- **Disclosure:** There must be a way for an individual to find out what information
about himself or herself is in a record, and how it is used.

- **Secondary Usage:** There must be a way for an individual to prevent informa-
tion about himself or herself, which was obtained for one purpose, from being
used or made available for other purposes without consent.

- **Record Correction:** There must be a way for an individual to correct or amend
a record of identifiable information about himself or herself.

- **Security:** Any organization creating, maintaining, using or disseminating
records of identifiable personal data must assure the reliability of the data for
their intended use and must take precautions to prevent misuse of the data.

By the late 1970s, information and communication technologies were facilitating
a growing global trade in, and processing of, personal data. As various countries
passed laws restricting the unlawful storage of personal data, the storage of inac-
curate personal data, or the abuse or unauthorized disclosure of such data, wor-
ries arose that global trade would be constrained by the growing patchwork of
national laws. In a far-sighted initiative, members of the Organisation for Economic
Co-operation and Development (OECD) came together and agreed to codify a set
of principles that might serve as a framework for countries to use when drafting
and implementing their own laws. The result was the 1980 OECD Guidelines on the

Protection of Privacy and Transborder Flows of Personal Data, a document which expressed and described eight “fair information practices” as follows:

- **Collection Limitation Principle:** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

- **Data Quality Principle:** Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and current.

- **Purpose Specification Principle:** The purposes for which personal data are collected should be specified no later than at the time of data collection, and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes, and as are specified on each occasion of change of purpose.

- **Use Limitation Principle:** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle except:
  - with the consent of the data subject, or
  - by the authority of law.

- **Security Safeguards Principle:** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure.

- **Openness Principle:** There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of stored personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

- **Individual Participation Principle:** An individual should have the right:
  a) to obtain from a data controller or equivalent, confirmation of whether or not the data controller has data relating to him or her;
  b) to have communicated to him (or her), data relating to him (or her) within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him (or her);
  c) to be given reasons if a request made under subparagraph (a) or (b) is denied, and to be able to challenge such denial; and
  d) to challenge data relating to him or her and, if the challenge is successful, to have the data erased, rectified, completed or amended.
Accountability Principle: A data controller should be accountable for complying with measures which give effect to the principles stated above.

Since 1980, these voluntary “fair information practices” (FIPs) have been widely adopted around the world in statutes, standards, codes of practice, information technologies, and in norms and common practices. In Canada, for example, businesses, consumers and the government agreed to adopt a comprehensive set of privacy practices, known as the Model Code for the Protection of Personal Information (CAN/CSA-Q830-96), which was subsequently incorporated in its entirety into Canada’s private sector privacy law. In the U.S., since the early 1970s, each successive government has remained committed to monitoring the “information practices” of organizations or, more specifically, the methods in which these organizations collect and use personal information and the safeguards they employ to ensure those practices are fair and provide adequate privacy protection. The result of this government intervention has been a series of guidelines and model codes that now represent commonly accepted principles, more formally known as Fair Information Practices (FIPs). Common throughout the U.S., FIPs are five core tenets of privacy protection that have proven both successful and enduring:

- Notice/Awareness;
- Choice/Consent;
- Access/Participation;
- Integrity/Security;
- Enforcement/Redress.

The most essential principle of the five is the first: Notice/Awareness. Consumers need to have knowledge of an organization’s privacy and information policies before any personal information can be collected and stored by that organization. This practice specifically protects consumers: without such proper notice, they cannot make any reasonably informed decision regarding the use and disclosure of their personal information. Furthermore, the other principles are only relevant when the consumer has knowledge of an organization’s information and privacy policies, and his or her rights as a consumer with respect to those policies. But despite this harmonization, significant variations persist in American law: the OECD Guidelines provide a floor, not a ceiling, for privacy protection.

Regardless of specific interpretation or manner of implementation, the OECD Guidelines and other similar FIPs accomplish two functions:

- They establish and confer broad rights on individuals, or data subjects, with respect to the collection, use and disclosure of their personal information by other parties.
They set out broad responsibilities and obligations of organizations in respect to
the collection, use and disclosure of personal information held in their custody.

The first function is commonly known as information privacy: the right or ability of
individuals to exercise a measure of control over the collection, use and disclosure
of their personal information by others. The second is data protection: the re-
sponsibility of organizations that collect, use, and disclose personal information to
abide by an externally established set of rules.

It is important to understand the distinction between the two functions. The first
approaches privacy from the perspective of the individual data subject, the sec-
ond from the perspective of the custodial organization. Good privacy laws and
data protection seek to reconcile the interests and objectives of both parties, but
new technologies typically upset pre-existing balances.

What is personal information? Many organizations mistakenly believe that personal
information is limited to basic “tombstone” data provided directly by the individ-
ual such as name, address, phone number, socioeconomic details and so forth.
Although statutory definitions vary around the world, personal information can in-
clude far more than this, such as:

- Any information associated or linked to an identifiable individual (e.g., per-
  sonal preferences, beliefs, opinions, habits, family and friends);
- Physical and biological attributes (photo images, genetic data);
- Account numbers and any unique identifiers associated with an individual;
- Transaction data (record of sales, customer service requests, returns logins,
  phone calls);
- Transaction data of devices registered to an individual (phone numbers, com-
  puter logins, location data);
- Information about an individual provided by third parties (credit reports, em-
  ployment references); and
- Information inferred, derived, or generated from data held about an individual
  (profiles, scores).
1.0 New Boundaries, New Business Processes

1.1 Context
As companies become inter-networked, they share new kinds of information. Given that the ONE is increasingly global, as networks expand across national as well as statistical boundaries, the risks associated with information sharing increase: information may be shared between companies with different laws governing their treatment of and responsibility to consumer privacy.

In addition, ONE business processes are necessarily characterized by dense inter-connections and constantly evolving relationships with a variety of internal and external partners, agents, affiliates and contractors. This modular approach to business affords high degrees of flexibility and adaptation to changing business environments and strategies. It also demands that the ONE focus on its core strengths.

Privacy and the ONE

Corporate Boundaries, Processes: How can privacy be protected in a business Web? Will the ONE’s modular, flexible approach to operations obscure or diminish accountability for unauthorized uses of customer data?

Modus Operandi: When employees become empowered to make decisions and try innovative approaches, will the devolution of authority diminish or enhance overall responsibility for, and adherence to, organizational policies intended to respect customer privacy? Conversely, will heavy-handed workplace surveillance measures and practices discourage employee initiative?

Relationships: Will the ONE go beyond traditional top-down approaches to engage and collaborate actively with clients, fostering what we describe as customer managed relationships?

Information Liquidity: How will the ONE manage the privacy risks associated with reliance on externally networked personal information and automated decision-making?

Technology: Will the ONE steer clear of temptations to use new technologies to collect excessive personal information from customers and employees?
1.2 Privacy concerns: outsourcing and offshoring

Personal data are increasingly handled by third party participants in information networks, and they are dealt with through outsourcing or offshoring practices. In general, “outsourcing” occurs when a company contracts out work to another company. “Offshoring” involves moving the work to another country, whether to a captive entity (i.e., a firm subsidiary) or to a third party supplier.2

Such third party data relationships are everywhere; now few businesses can survive without relying on other firms to help provide, process, or manage data. Whether exchanging data with business partners or sharing information internally, each transaction between businesses establishes a data relationship. These relationships must be carefully managed to ensure compliance with both an organization’s policies and applicable external regulations around data protection.

In a b-web, information security is only as effective as the weakest link: “If one trading partner has a poor identity management program, another never tests its disaster recovery plan, and a third does not regularly assess its information technology outsourcer’s compliance with information security policies, one’s own security posture cannot logically rise above the lowest point achieved by these other entities.”3 As more organizations collaborate intimately, it becomes increasingly difficult for senior management to fully identify and manage the larger organization’s ever growing risk interdependency. Collaboration has changed the security landscape; the behaviour of a single organization can have a wide-ranging impact on other b-web participants. Senior managers may think their organization is adequately protected when in reality their investments are undermined by process flaws. The statistic of such potential breaches is cause for concern: according to an Ernst & Young global survey, 80 per cent of respondents failed to conduct a regular assessment of their IT outsourcer’s compliance with the host organization’s information security and privacy regulatory requirements.4

Reported information security breaches are occurring with increasing frequency, severity and cost to businesses.5 Organizations are understandably reluctant to report data security incidents, for fear of the negative effects on their competitive stance, public image and stock value. This reluctance is being trumped now by

---

new accountability laws and regulations containing mandatory reporting requirements. Quite often, firms are not even aware that data security breaches have taken place if they occurred among business partners and affiliates. New data governance and similar compliance rules will strip firms of any reluctance to assume greater responsibility for and control over the actions of others.

The risks of outsourcing are thus known to be significant: it takes only one incident to damage years of brand building, and with the corporate identity go the trust, loyalty and business of customers, regardless of who is technically or legally liable. One cautionary tale of the risks of insufficient privacy monitoring involves a large national bank that outsourced its customer care and call centre operations to a vendor in the Ukraine.⁶ The company concluded contracts with the vendor to ensure that it took full responsibility for complying with all U.S. regulatory requirements, as well as with the bank’s own privacy policy, which included a strict do not share with third parties for secondary uses without a consent clause. The Ukrainian vendor also contracted to comply with strict data protection and information security requirements as per the U.S. Federal Trade Commission’s Safeguards Rule. Nine months after operations began, thousands of U.S. customers began receiving charges on their credit card statements for magazine subscriptions and online services that they had never purchased. Hundreds complained that they became victims of identity theft, apparently a result of information leaks. A few customers reported that their entire bank balances had been transferred to untraceable locations. In response, the bank hired a forensic expert to determine where the possible data leak could have occurred. It was eventually discovered that the leak had transpired at an offshore outsourced location. It was traced to a new employee of the Ukrainian vendor who had remote access to the company’s data warehouse. Notably, investigators found that the vendor’s IT director had known about the leak months before the incident occurred, but never bothered to report it.

Such risks are not limited to offshore operations; companies should also determine whether domestic partners observe adequate security standards. In March 2005, for instance, the Federal Trade Commission recently settled a case in which a company that sold a shopping cart application to a Web merchant then provided customer information to other entities, contrary to the merchant’s privacy policy.⁷ The Web company had failed to ensure partner compliance before signing the contract.

The challenges to ensuring that security standards are met and maintained are significant. The average *Fortune* 500 company typically has over 10,000 contracts and agreements with partners, affiliates, contractors and other third parties, all of

---


whom affect the treatment of personal information. Just understanding data assets, uses and flows can thus be a daunting task, let alone subjecting these assets, uses and flows to clear and comprehensive policies, and enforceable procedures.

At the heart of the debate over privacy is the issue of corporate accountability. Organizations that are most visible or proximate to affected individuals bear most of the negative publicity and criticism for privacy breaches. When a privacy breach occurs, it will matter little to the public that the breach actually occurred at a partner's e-commerce payments processing website platform located in another jurisdiction; the organization that the customer deals with directly bears the most accountability and risk. As the most visible target, such an organization can suffer from diminution of brand and loss of credibility and sales, or by incurring the high costs of litigation, compensating victims, re-engineering information systems, or submitting to extensive audit and certification processes. When it comes to allocating blame, public perception can override corporate reality, and therefore the proximate organization must have the strongest incentive to ensure that personal information is managed responsibly.

1.3 Recommendations

Offshoring, outsourcing and third party data relationships pose significant challenges to the governance of personal information. Meeting these challenges requires coordinated and ongoing management of multiple elements of data policy compliance and risk management across all entities in the data sharing relationship. These elements include risk assessment, monitoring of the sharing relationship and prospective third parties, and substantial monitoring, tracking, classifying and regulation of enterprise data flows. But there is no one-size-fits-all solution; the data collection, storage, use, sharing, oversight and enforcement needs of every firm are unique. We do know, however, that a comprehensive approach is more likely to be successful; one that accounts for people, processes, systems and policies.

Any solution must begin with a regulatory review: numerous laws, both current and proposed, restrict or impose conditions on offshoring and outsourcing activities. According to Alan Westin, founder of Privacy and American Business, provisions for protecting personally identifiable information will play a major role in anti-offshoring bills at federal and state levels. A significant data breach or identity theft scandal in just one overseas location could jump start legislative responses. Ignorance of the law, including potential laws, will be no defence.

Legal requirements regarding the treatment or sharing of personal data will determine the ways in which risk is assessed, and the choice of assessment instruments and approaches. Europe, for example, prohibits transborder personal data flows unless certain “adequacy” requirements are satisfied. In the U.S., firms that outsource are already governed by numerous laws and regulations that impose compliance requirements, such as the Sarbanes-Oxley Act, the Health Insurance
Portability and Accountability Act (HIPAA), the Gramm Leach Bliley Act, and the Fair Credit Reporting Act.

Outsourcing that involves personal data in particular has recently been drawing attention from regulatory bodies and the general public. Some state laws require that companies choose domestic over foreign workers to process employee data, while other states require disclosure if work on government contracts is undertaken outside the U.S. Maryland and Massachusetts vetoed similar bills in 2004, but it is expected that those bills will return. There are currently 115 anti-offshoring bills pending in 40 states; the majority aim to limit work contracted out by the state. Many aim also to prohibit state aid for overseas outsourcing, enforce disclosure of call centre locations, restrict outsourcing of personal sensitive data such as health or financial, and in some cases to require consent from customers.

California’s legislature passed five anti-offshoring bills in 2004. Protective measures included allowing no state contracts for work performed outside the U.S. and no outsourcing of Social Security Numbers, driver’s licences and personal health data. One particular law required overseas call centres to disclose their location to residents of California and local employers to report to the state if they moved operations offshore. Governor Schwarzenegger ultimately vetoed all five bills, but the backlash was significant; it is likely that these bills will re-emerge for a second attempt.

Regulations exist at the national level as well: the U.S. Senate passed the Dodd Bill in 2004, which prohibits the awarding of federal contracts to companies with overseas employees. A proposed House resolution also seeks to enforce consent prior to transferring sensitive personal data to countries that lack adequate privacy protections as defined by the Federal Trade Commission. Hillary Clinton’s proposed “Safe ID Act” will prohibit businesses from processing sensitive personal information in foreign countries without offering an opt-out choice to the public. In addition, if the Act passes, businesses will become directly liable for any privacy breaches.

In such an environment, rules for data flows and uses should comply across all jurisdictions to established international benchmarks, like COBIT® and ISO 17799. Adherence should be monitored through due diligence, site visits, contractual remedies and third party audit and certification.

To manage an ONE effectively, a company must develop a comprehensive set of objectives and policies regarding privacy and security of data uses and flows. These policies must be clearly expressed and effectively communicated throughout the ONE and to all third parties. Some elements to consider:

---

Minimize data collection, use and security among partners;
Develop strong contractual agreements and deterrents for third parties;
Deploy continuous monitoring, auditing and enforcement mechanisms;
Implement privacy crisis management protocol in the event of a breach; and
Develop adequate consumer trust to draw upon in the event of an incident (customers may be more forgiving).

Information and communications technologies (ICTs) can also help maintain security for consumers: firewalls and other filtering software, secure transmissions, handling and storage of data, strong authentication, access controls, extensive logging and audit trails, and other safeguards can be assured in part through ICTs, and can significantly increase consumer security. It must be remembered, however, that a critical element of success fully deploying such systems involves comprehensive education, training and awareness programs for all employees involved in these processes.

With regard to transparency, current U.S. legislation requires firms to disclose their outsourcing policies and practices to customers. Knowing that customers will be informed about outsourcing arrangements might motivate companies to make sure those arrangements are secure. One U.S. financial company, E-Loan, not only explains its outsourcing practices to its customers, but actually offers them a choice of whether they would like their financial arrangements processed in-house.

### 2.0 Modus Operandi

#### 2.1 Context
The modus operandi of the ONE is characterized by flatter hierarchies, greater collaboration, devolved decision making, more risk taking, high flexibility, agility, adaptability, and innovation.

#### 2.2 Privacy concerns: the insider conundrum vs. internal surveillance
In such collaborative environments, organization-wide privacy and security policies governing the use of data can be difficult to implement and enforce. Because such policies are often mandated from above, their hierarchical quality may conflict with the more open, collaborative culture of the ONE. Often such policies are perceived as barriers to new and innovative thinking, products and practices.

At the same time, flatter, decentralized organizations may be well-connected, but they are also more vulnerable. The more that senior management has lost its situational awareness (the degree of accuracy by which perception of the current environment mirrors reality) the less likely it will be able to comprehend the
organization’s ever growing interdependence. Single events can have profound impacts that cascade across the network. Furthermore, when individual employees are empowered, how do you ensure that they respect privacy policies and principles? How do you ensure that data is protected? If everyone is responsible for privacy and security, then perhaps no one is.

Recent data privacy and security breaches have focused the public and lawmakers’ attention on the poor information management practices and procedures of businesses, especially since large-scale losses and theft of personal information can have profoundly negative effects on innocent individuals.

2.3 The insider conundrum

It is not uncommon for marketing and communications departments, in the pursuit of quarterly objectives and hard metrics (and when given a free hand), to develop initiatives that bypass privacy policies. In their efforts to ensure security, IT departments want to control and lock down all information assets, often by filtering and logging everything, or otherwise engaging in what could be perceived as nosey employee surveillance practices. Software development teams may add invasive privacy and security features to products that act as spyware. Overzealous human resources departments, looking for the perfect employee, may carry out deeper background checks than necessary or engage in psychological profiling. Any of these activities can land a company in hot water.

Sometimes personal data exposure or misuse occurs by accident, such as when pharmaceutical giant Eli Lilly accidentally exposed the email addresses of 669 Prozac users in the “To:” field of an email marketing solicitation, resulting in an FTC investigation and settlement, as well as a tarnished brand and reputation.10 Quite often, such data loss or unauthorized exposure occurs as a result of negligence or failure to follow simple policies and procedures, such as when laptops with unencrypted personal data go missing, or when default passwords are not changed.

Inside theft is a big problem. It is well known that insiders who access databases often have network authorization, knowledge of data access codes and a precise idea of the information they want to exploit. Surprisingly, most database applications even sophisticated high-end ones store information in “clear text” that is completely unprotected.

10 “Even the unintentional release of sensitive medical information is a serious breach of consumers’ trust,” said the Director of the FTC’s Bureau of Consumer Protection. “Companies that obtain sensitive information in exchange for a promise to keep it confidential must take appropriate steps to ensure the security of that information.” http://www.ftc.gov/opa/2002/01/elililly.htm
Further, there are more unauthorized accesses to databases than corporations admit to their clients, stockholders and business partners, or report to law enforcement. Gartner estimates that internal employees commit 70 per cent of information intrusions, and more than 95 per cent of the intrusions result in significant financial losses. A 2002 survey of 163 Fortune 1,000 companies found that 70 per cent of reported security breaches were linked to insiders.  

Another survey by the Computer Security Institute revealed that over half of all corporate databases have some kind of breach every year, and the average breach results in close to $4 million in losses. And these are just the security problems that companies report!

Non-technical and behavioral forms of intrusion are also common. What makes the insider threat so daunting is that most breaches do not require sophisticated methods, and they most often occur on site during normal working hours by employees, freelance contractors, employees of corporate contractors, and even clients. In some cases, disgruntled employees simply wish to hurt an organization and its reputation.

Finally, there are the security problems associated with external hackers, thieves, and con artists. Why steal one identity from a trash bin when you can steal a million from an insecure database?

Consider some recent breaches:

- Time Warner reported that a cooler sized container of computer tapes containing personal information of 600,000 current and former employees was lost on its way to a data storage facility in March 2005. The computer tapes contained the names, SSNs, and other data pertaining to current and former employees dating back to 1986.
- Data broker ChoicePoint reported the unauthorized access of over 150,000 detailed dossiers by scam artists over a period of a year. At least 700 known instances of identity theft resulted from this security breach. Poor access control and authentication procedures were blamed.
- Online brokerage Ameritrade disclosed in April 2005 that it had lost a backup computer tape containing records of 200,000 customers.
- A former employee of a Washington area Blockbuster Video store was indicted on charges of stealing customer identities and using them to buy more than $117,000 in trips, electronics, and other goods, including a Mercedes-Benz.


• LexisNexis reported a privacy breach in its Seisint database division. Hackers accessed more than 300,000 profiles, including SSNs and driver’s licence numbers more than 10 times the number originally reported. The company blamed poor access management practices.

• A California medical group is currently informing nearly 185,000 current and former patients that their financial and medical records may have been compromised following the theft of computers containing personal data.

• Health-care giant Kaiser Permanente notified 140 patients that a disgruntled former employee had posted confidential information about them on her blog.

• Tokyo Disney amusement parks reported that personal information on 122,000 customers who bought one year admission passes in 2002 was leaked. Several hundred received fraudulent phone calls or direct mail.

• Bank of America admitted it lost backup tapes containing personal information on 1.2 million federal employees, including several Congress members.

This string of high-profile data security breaches has sparked a public firestorm and closer lawmaker scrutiny of businesses’ information management and security practices. A flurry of proposals at federal and state levels intends to ensure that businesses assume more responsibility and liability as custodians of personal data.

In response, businesses have invested heavily in information security. A significant and growing percentage of corporations routinely monitor employee behaviour and activities such as Web surfing and email use. We are seeing a strong surge in interest and demand for identity management, authentication, and role based access systems that track and monitor virtually every employee activity.

The concept behind these security efforts is clear: information is an asset, and access needs to be controlled and predicated on strong identification, authorization and auditability.

Strong security enhances privacy, but this trend seems counter to ONE culture. We are seeing a rise in employee litigation against companies in reaction to excessive monitoring and surveillance. Employee privacy is being pitted against customer privacy and employees are losing.

The fundamental problem, again, is ensuring accountability and governance of personal data while respecting the privacy of customers, data subjects and employees. The rogue actions of some empowered staff, however well-intentioned, can have negative effects on the entire organization. At the same time, a heavily monitored and restricted workforce can become less empowered and more resentful, ultimately to the detriment of the ONE.
2.4 Possible solutions

As with any information privacy and security program, there is no one-size-fits-all solution. Every organization is unique, and a lot depends on the nature of the business, the personal information at stake, and the degree of vulnerability and risks involved.

A continuous privacy awareness and training program for employees is a requirement for success. In fact, the most successful ONEs have well developed corporate cultures of customer privacy and respect for employees. Clear and comprehensive privacy policies, effectively communicated and enforced, ensure that privacy and security are infused throughout the organization and promoted as everybody’s responsibility. It is also not uncommon for performance appraisals and bonuses to be tied to adherence to corporate privacy policies. At the same time, clear and consistent policies on employee surveillance, communicated well and carried out in a fair and impartial manner with appropriate curbs on potential abuses, can go a long way in dissipating employee fears, resentment, and counterproductive behaviour.

Privacy and security leadership is also a necessity: firms require a strong chief privacy officer (CPO) who understands all aspects of the organization and is capable of navigating and working with all departments. When vested with appropriate oversight and/or veto authority, such an individual can become a champion for privacy within an organization, be able to bridge the divides between higher and lower management and between different corporate divisions, and become the “go to” person whenever there are questions or incipient problems. A champion for strong data privacy and security, the CPO can also put in place credible and effective policies governing the use of workplace monitoring technologies without raising employees’ concerns about excessive surveillance. A good CPO can reconcile the apparent contradictions between strong data security and employee privacy on the one hand, and the operational needs of the ONE on the other, thereby fostering a climate of trust and collaboration.

Perhaps most significantly, and today more than ever before, the CPO uses new technological tools and automated mechanisms. For example, new database and data flow “discovery tools” can map organizational information flows and minimize security risks by automatically detecting and responding to possible data misuses at the earliest possible stages through heuristic intrusion detection systems. Similar tools exist to evaluate website compliance to privacy and security standards. There has also been a growth in interest in enterprise identity management, access control and automated content filtering systems.

Just as inbound electronic communications can be scanned for viruses and inappropriate content, so too can outbound messages be scanned for protected intellectual property and “leakage” of sensitive personal information. Best of all, these tools can be automated so that “surveillance” need not be arbitrary or performed by a human, except when suspicious incidents are flagged for follow-up.
The emergence and growth of data security technologies and systems has been remarkable. Such technologies are far too numerous to mention here, but a knowledgeable CPO or Chief Information Officer, would be well aware of the latest data security systems.

Technological tools can also be effective in establishing audit trails. One promising solution is to attach a “condition of use,” such as client privacy preferences, directly to the data, so that privacy and security policies are effectively “bound up” with the data the client supplies. The rules relating to data use are “wrapped around” the data itself. In this way, many data privacy and security policies can be demonstrably self-enforcing, with little or no need for direct CPO intervention or oversight. IBM’s Tivoli Privacy Manager is one such successful tool.13

2.5 Summary
As information needs continue to grow, so too will the challenges of complying with a widening range of anticipated regulatory privacy and security requirements and public expectations. A strong culture of privacy and security, and of employee respect and trust, is the foundation for a successful ONE. To maintain agility and flexibility, an empowered Chief Privacy Officer is needed to install the proper mix of policies, procedures, training and technologies that will serve both to manage personal data throughout the ONE’s life cycle and to assure employees that they are not being unfairly watched.

3.0 Relationships

3.1 Context
The success of a company’s ONE is a function of positive experiences and strong relationships with customers. Word of mouth endorsements are among the most valuable types of marketing any organization can have, and by providing useful, efficient, personalized services and products, the best companies foster enduring trust, loyalty and repeat business. So valuable is the repeat value of a customer that, increasingly, products are given away at discounted prices in favor of establishing a long-term relationship.

3.2 Privacy concerns: consumer trust
In today’s hyper-competitive climate, brand and reputation are shorthand vehicles for conveying trusted information, and fostering and reinforcing positive experiences with customers. Trust takes a long time to build, but a short time to erode and lose. Trust is built by making and keeping promises over time, and being transparent and reliable about your commitments and policies.

In order to build a more intimate relationship with consumers, businesses are adopting novel techniques to serve customers with personalized services, such as discounted loyalty cards. Integrated customer relationship management (CRM) technologies provide holistic views of customers, their data and their transaction histories, while providing customers with convenient single-window “no wrong door” portals for efficient service.

We are seeing a trend towards relationship and permission-based marketing in an effort to engage the customer in an ongoing, personalized, customized, 1:1 manner. Such marketing techniques depend on collecting and collating as much information as possible about the client in an effort to differentiate, understand and respond to clients’ specific needs and wishes (ideally before they themselves recognize this!).

Permission-based marketing may result in less data than that obtained through arbitrary online registrations, but the information thus collected is, without a doubt, far more relevant. Further, permission-based marketing also builds loyalty through trust. To use an analogy, a lot more can be accomplished with a sniper’s rifle than a shotgun. A case in point: a 2003 survey of over 1,000 persons across the United States found that 70 per cent of respondents were willing to receive legitimate email marketing messages provided that they had given their consent.

In the spring of 2005, Ipsos-Reid conducted a survey that reported that the number of respondents willing to receive commercial email was increasing, again with the caveat that they had given their permission. The survey found that close to 80 per cent of Internet users have registered to receive email from an average of nine commercial websites. Combined with the latest email filters, Internet users can now customize their choice of exactly which companies are allowed into their inbox, and who goes directly to the trash file.

Thin Data, a Toronto based email service provider, began a permission-based marketing campaign on behalf of Mirvish Productions, a theatre production company in Toronto, Canada. Thin Data sent a monthly email newsletter to over 15,000 subscribers and found it was read by 65 per cent of recipients per month. In comparison, it found that less than 30 per cent of recipients of indiscriminant direct mail campaigns opened emails.

---

17 Ibid.
Permission-based marketing, suggests Seth Godin, is like dating. The company or marketer approaches the consumer to request a date. If the consumer says yes, they go out, and if both parties are interested, self-disclosure of personal details takes place. Trust builds over time, and the relationship may continue, perhaps for years, and in some cases, a lifetime.

Building on the idea of permission-based marketing, the concept of the “Customer Managed Relationship” (or CMR instead of CRM) has emerged, where the customer manages the relationship with the company and controls his or her own data. The most popular industry view holds that customers should own their own personal profile and have access to all the information about themselves across all departments. Additionally, the CMR system should be designed around consumers’ needs and desires. An example of this would be Vivendi Universal’s Universal Music Mobile, launched in 2001 as one of the first CMR-oriented services offered. The Mobile provides an assortment of music-related multimedia services, and self-service, combined with the billing program, is a major feature of the service: it allows customers to activate multiple services and features online, view their usage, pay or pre-pay online, change service options online, modify their contract, or change billing details themselves. Vivendi Universal took a relatively early lead in letting its customers define how they wanted to communicate with the company, not the opposite. In this kind of relationship, consumers feel a sense of empowerment and control (which equals a feeling of trust and security) over their personal information. IBM Chief Privacy Officer Harriet Pearson refers to this kind of relationship as a “trusted balance” – a willingness to communicate and put into effect a concise set of privacy rules. Also crucial is the fact that this arrangement is about selling an emotion or an experience, the same way that Nike sells an athletic lifestyle. The key to success in a CMR is thus allowing customers not only to feel in control of their choices as consumers, but also to be able to monitor and manage their own personal information if they participate in a CMR by choice, it is a sure sign they trust the company.

But despite growing privacy protocols, people are increasingly wary about disclosing unnecessary information about themselves. If customers think information requests are superfluous, intrusive or unnecessary, they may lie or abandon the process. “Relationships” that are not founded upon genuine dialogue, reciprocity and negotiation can flounder, such as when privacy promises are obscure and written in vague non-committal legalese (and subject to change at any time). Even worse is when the defaults are invasive or perceived to be disrespectful of customers’ wishes, such as when a website’s registration default is “optin.”

As far as youth are concerned, it would be in error to dismiss them as apathetic when it comes to concern over privacy. The 2004 Harris Interactive survey of youth found that many of them do in fact care. The degree of concern with “privacy being invaded online” varied by age, with the lowest being eight- to nine-year-olds at 25 per cent, and the highest being 18 to 21-year-olds at over 50 per cent.20

“Privacy hawks,” as dubbed by Ben Charny, engage in “privacy self-defense” by employing guerilla tactics to protect their personal information.21 The Pew Charitable Trust describes these cyber renegades as most likely male, with over a third between the ages of 18 to 29, who have been online for three or more years and make up 25 per cent of the Internet population. While by no means a homogeneous group, they hold one common belief: their personal information will ultimately be exploited and “privacy policies” are not always to be trusted. Therefore, they feel that falsifying their personal information is necessary out of self-defence.

In terms of specific tactics to maintain personal privacy, the most common is to simply lie. Those who are aware of a website’s limitations understand that they can, with impunity, provide completely false information on a registration form to qualify for access. For some it is even a game of sorts: one can declare oneself as a CEO who lives in Beverly Hills and makes between $0 and $15,000 per annum. Indeed, it would not be surprising to find that the most common Zip code entered on website registration forms is 90210, from the popular 1990s television show, or that Bill Gates has registered with MSN more than one hundred times.

To date there has been only a handful of in-depth studies conducted on individuals who lie when registering online. In 2000 it was found that 20 per cent to 30 per cent of registrants lied (with teenagers being the highest scoring age demographic), but this is considered a conservative estimate.22 the main reasons cited for lying included distrust over how personal information would be used, avoiding junk mail, and a desire to remain anonymous. This desire for continued privacy is something to take into account when considering the ROI of advertising and marketing budgets.

Another growing method of consumer self-defense is having a secondary, or “disposable,” email address. Anyone can log onto Hotmail in five minutes and create an email account based entirely on false information. A 2004 Harris Interactive survey found that youth aged 10 to 21 had an average of two to three email addresses.23 Some websites such as Dodgeit, Mailinator, Spamgourmet and Spambob now even

20 Harris Interactive, Youth Pulse, June/July 2004, p. 64.
23 Harris Interactive, Youth Pulse, June/July 2004, p. 53.
offer free disposable email accounts. In the Spring of 2005, Spamgourmet.com reported that it had almost 90,000 subscribers with nearly 1.5 million disposable email addresses. The Pew Internet and American Life Project found that 20 per cent of persons who use the Internet have used disposable email addresses, while the number of teenagers who did the same was as high as 56 per cent. It should also be noted that disposable email addresses are not only used to avoid junk mail; they are also a safe vehicle for entering contests, or registering for free gifts or rebates (the address is disposed of once the contest is over, or the gift or rebate has been received).

Privacy hawks and anyone else who wants to remain anonymous online have received help from advances in Internet technology. Mozilla Firefox is an Internet browser that allows for anonymous surfing. Most browsers now include toolbars equipped with a function that blocks pop-up ads and cookies. And almost all email services now come with “block sender” and “junk mail” options that automatically vet email. There is also a host of commercial and free software programs available, such as Ad-Aware and BetaSpyware, that provide real-time defense against unwanted intrusion from hackers and marketers, and other forms of surreptitious data gathering. In fact, these features are becoming so commonplace that disposable email addresses may soon be redundant, because even if unwanted contact is made, a simple click of a button can ban a marketer or advertiser indefinitely. As of April 2005, Ipsos-Reid reported that 77 per cent of Canadians already use such filters while online.24 In 2003, the Pew Internet and American Life Project found that 37 per cent of Americans used filters while online.25 In 2005, the number of families with teenagers in the U.S. that used online filters at home was found to be 54 per cent, up from 41 per cent in 2000.26

Self-defence of personal privacy is a growing movement, no longer limited to the actions of a few privacy hawks. People are becoming more and more organized; they are becoming connected in their common goal. Strategies, techniques, and tactics in defence of one’s privacy are now becoming widespread topics of conversation in chat rooms and on blogs.

Microsoft’s small business website offers a top-10 list for successful permission based email marketing, with number 10 being always remember the network effect. “Bad news travels much faster than good on the Internet. An angry online customer can broadcast his ire to millions by creating an ‘I hate [your company]’ website, emailing an account of their experience to friends, posting it on message boards and other ways. Remember, in this economy the customer is in

---

control.”

For further reading on anti-company websites, Forbes.com has published an online article featuring the top corporate “hate” websites.

### 3.3 Possible solutions

Strong, clear and overt privacy commitments, honored over time, demonstrate respect for the customer and foster trust and loyalty.

Customer knowledge and consent should be prerequisites for all marketing activities. The customer should be given every opportunity to become a participant in the marketing process, and to provide feedback and direction. New technologies make it possible for organizations to give their customers direct access to all data held on them, as well as other self-serve options.

Trust and brand are easily eroded when privacy commitments are not perceived to be honored, or when the client is denied meaningful opportunities to be a participant in the “relationship.” Let CRM morph into CMR!

When it comes to personal information, not sharing is caring. Your customers will thank you. Successful companies need to take a long-term strategic view of value of their customer data and resist the temptation to share it or sell it to third parties without their customers’ consent.

Conversely, people will not lie when they feel there is a trusted connection between themselves and a company. They will almost invariably give their personal details if they think a relationship with a particular company is going to benefit them, even if all they want is to stay informed of the latest trends on products and services of interest. And isn’t that precisely what you want to pitch to them? Find out what your customers want and give it to them they will keep coming back for more. But give them what they do not want and you will drive them away. You decide.

*Your privacy mantra should be, “Always ask, never assume.”*

### 4.0 Information Liquidity

#### 4.1 Context

An ONE aggregates data from disparate third party sources to create business intelligence that, in turn, may overlap with personal information. Many public databases contain private information that firms can easily access. How can privacy be protected?
4.2 Privacy concerns: bad data, bad decisions

“Search, don’t sort” is Google’s motto and advice to customers. This advice is particularly apt at a time when technology provides individuals and firms with the ability to instantly find, aggregate and distill a virtually unlimited quantity of information for novel uses and competitive purposes.

Taking advantage of this new wealth of data, a new and rapidly growing industry has arisen to collect, analyze, and sell aggregated personal information and profiles. The types of companies that do this are varied, such as TransUnion and Experian, which are credit bureaus to LexisNexis, and most notably ChoicePoint, which is described as a data miner and aggregator. By far, ChoicePoint is the largest data aggregator on the market, with billions of public records in its database.\(^2^9\) With data that includes motor vehicle registrations, license and deed transfers, military records, names, addresses and SSNs, ChoicePoint routinely sells dossiers to police, lawyers, reporters, private investigators and even to the U.S. Department of Homeland Security.

The direct marketing industry has been transformed and spurred on to new heights by the online environment, where all manner of technologies are being deployed to collect highly granular personal information that is then combined with data available elsewhere and used to profile and predict behaviour. Examples of these technologies include use of “cookies,” “Web bugs,” and other electronic tools and agents that track online activities.

Attempts to consolidate information is not always successful, however: for instance, online advertising giant DoubleClick’s attempt in 1999 to purchase Abacus Direct for $1 billion in order to merge data on Net surfing habits from the five billion ads DoubleClick served per week and the two billion personally identifiable consumer catalog transactions recorded by Abacus was vigorously opposed by privacy advocates and consumers on privacy grounds, prompting a three-year investigation by the FTC. The deal ultimately failed.

Personal consumer information is incredibly valuable to corporations: when Air Canada fell into bankruptcy proceedings, the airline sold off its information assets, which consisted of millions of profiles of Aeroplan members from its popular loyalty program, for nearly CAN $1 billion about three times the market capitalization of the company’s airline fleet.

So lucrative is the information profiling industry that online marketers have formed numerous lobby groups and associations such as Network Advertising Initiative (NAI) and Online Privacy Alliance (OPA) in order to help shape the evolution of new laws and regulations that could have a direct impact on their business models.

Bob Sullivan, “Database giant gives access to fake firms,” MSNBC, February 14, 2005
http://msnbc.msn.com/id/6969799
The marketplace for personal information is estimated to be in the tens of billions of dollars per year in the U.S. alone, with businesses as the main customers. In the past six months, several new books documenting the extent of the information aggregation and profiling industry have hit the market. Among the best are The Digital Person: Technology and Privacy in the Digital Age,\textsuperscript{30} by Daniel Solove, and No Place to Hide, by Robert O’Harrow, Jr.\textsuperscript{31}

Personal information is collected and sold to firms for a fast growing variety of purposes. Detailed dossiers on individuals are bought and sold like any commodity in a vast and growing “grey market” in order to carry out background checks, to authenticate people, credentials, and claims, to evaluate individual risk, to generate client profiles and make behaviour predictions, to establish metrics, for billing purposes, and for a wide range of “research” purposes, such as marketing and national security. Such information is routinely used by business to make decisions affecting individuals, such as whether or not to hire or promote them, or to grant them credit or insurance, and in general to establish the terms of a company’s relationship with an individual.

The availability and use of detailed dossiers on individuals, and the derived profiles or scores, is seen as beneficial to individuals and to society because it helps detect and deter fraud (e.g., in the form of employment background checks); it helps lower transactions costs (e.g., the “miracle of instant credit”); and it enables better servicing of customer needs (e.g., by providing customer profiles). The general goal behind tapping huge database grids is to make more informed, smarter decisions.

Unfortunately, too much personal information liquidity and automated processing can be a liability. The history of privacy in the 20th century has shown that the abuse of personal information collection often provokes public outcries, backlashes, and new regulations and liabilities for organizations that act as data custodians especially when individuals are negatively affected as a result.

We may in fact be witnessing a “perfect privacy storm” right now in the wake of an endless series of large scale privacy and security breaches reported almost daily in the news. Given the ever increasing incidence of identity theft, the public and lawmakers are beginning to demand that businesses begin to shoulder their fair share of responsibility for the many negative effects and costs that fall upon innocent third parties as a result of data mismanagement. New federal laws and regulations are widely expected within the year that will curb excessive business practices involving personal information collection, use and disclosure, and to arm individuals with better knowledge and greater rights of access and redress vis-à-vis those businesses that would collect and use their personal information.

\textsuperscript{31} Robert O’Harrow Jr., No Place To Hide, New York, Simon & Schuster, 2005.
As noted earlier, the excesses of the yellow press in the early 20th century spawned the concept of the right to privacy, and led to a variety of legal restrictions and tort remedies for affected individuals. Similarly, abuses of centralized state dossiers and financial credit reports led to the waves of law, regulation, and litigation intended to curb the activity and provide various rights to individuals. Today, similar concerns about the extent and accuracy of personal data contained in blacklists, especially those shared with and used by governments, are the subject of considerable public debate.

Moreover, high-profile stalking and murders (e.g., Rebecca Schaeffer, Amy Boyer) that were facilitated by access to sensitive personal information led to new restrictions and liabilities on the use and disclosure of sensitive personal information. A desire to protect children led to other controls on information about individuals under the age of 13. The negative effects and costs of spam, telemarketing and spyware are also provoking new controls. Most recently, the ChoicePoint data breach has focused the regulatory spotlight on the practices and liabilities of large “infomediaries” who collect and sell personal information. In February 2005, it was discovered by an internal employee of ChoicePoint that identity thieves, in a plot twist taken from a Hollywood movie, were creating false identities to establish accounts with ChoicePoint and then using those accounts to commit identity theft. The employee became suspicious when he noticed that applications from some businesses were coming from a nearby Kinko’s. ChoicePoint reacted by notifying close to 200,000 persons, as required by California law, that their personal information may have been compromised. However, the Los Angeles police department believes that as many as 500,000 persons may have been affected.32 As of April 2005, there are 39 bills (pending in 19 states)33 that are modeled after California’s SB1386, which is known for its clause requiring that persons be notified when their personal information has been breached.

There is growing sentiment among lawmakers to place more accountability and liability on those organizations that have used personal information in irresponsible ways. The FTC has shown a willingness to investigate firms that do not live up to their privacy promises and who otherwise engage in unfair and deceptive trade practices involving the use of personal information.

Common privacy issues and liabilities include the following:

- **Failing to inform or seek the permission of the customer to obtain personal information from other sources**, then collating with data provided directly by the customer.

32 Our Georgia History, ChoicePoint Scandal, April 2005
http://www.ourgeorgiahistory.com/chronpop/1000072

Failing to get explicit informed consent from the customer to share his or her personal information with third parties and other members of the intelligence network.

Obtaining and using old or inaccurate data obtained from third parties. If incorrect data are used to make decisions affecting an individual, the ONE must be prepared to justify its decision making and face the consequences when incorrect.

Automated processing and decision-making can also lead to discriminatory treatment of customers, with no recourse for action. For example, customers with “undesirable” phone numbers will wait long service times while “desirable” phone numbers get through to customer service right way. Who is accountable when customers are denied service because they have erroneously been placed on a secret networked blacklist?

Networked intelligence and automated decision making tools can be of a great service to the public, but a very real danger exists in that incorrect or outdated personal data can propagate throughout these systems. Again, accountability and responsibility are often diluted when personal data, and in this case, incorrect assessments, are available everywhere, instantaneously.

Companies that rely on other sources for their information and decision making needs must understand that they may nonetheless incur liability and penalties for failing to take responsibility for their actions.

4.3 Possible solutions
As the ONE increasingly taps into the grid of available personal data, it must ensure that this information is

- Legally acquired, used or shared;
- Sufficiently accurate for the identified purposes;
- Appropriate and proportional for those purposes;
- Used in a transparent and defensible manner; and
- Available for access and correction by the individual.

Organizations must be clear and up front about the nature and extent of their information activities involving third parties. For example, a considerable amount of sensitive personal information may be acquired from various sources in order to screen potential employees. The routine sharing and use of information among a large number of affiliates, partners, and subcontractors in the corporate “family” should be made explicit.
Firms should also always explain and justify the use of automated decision-making tools. Wherever possible, they should seek the informed consent of their customers, and be prepared to provide access and correction to all data about an individual (not just information supplied directly by the individual), along with an explanation of specific data items. If consent is withdrawn, then the request should be honored throughout the information supply chain, such as agreeing to remove an individual from a mailing list, for example. Increasingly, firms are required in many jurisdictions to provide, on demand, not just access but an account of all uses and disclosures of customer information.

Successful ONEs should strive to maintain and share only the most limited and accurate data or assessments about their customers with others, and should have in place mechanisms to deal with exceptions, corrections and other remedial processes. They should also take appropriate steps to ensure, and to demonstrate, that the networked sources from which they receive and supply customer data are reputable and trustworthy.

5.0 Technology

5.1 Context
Remarkable advances in information and communication technologies make it possible now, on a cost effective scale never seen before, to collect, store, process, and share vast amounts of highly granular personal data. This data become our digital shadows, proxies for the real thing, upon which organizations and governments alike will assess and make decisions both for and about us.

5.2 Privacy concerns:
Over collection and under disclosure
(the law of unintended consequences)
Just because technology lets you do something, should you do it?

It is generally accepted that the development and adoption of new technologies races far ahead of our ability to understand their consequences, let alone control them. Perhaps this is a good thing, since it gives lead time for experimentation and innovation, and at times, unintended consequences.

Organizations that are early developers or adopters of innovative information communication technology (ICT) often stand to gain an advantage over their competitors, especially in new areas and industries. Being an industry pacesetter, however, sometimes comes at the cost of working in grey areas of regulation, and incurring hard to quantify privacy risks and public backlashes. All of the major ICT innovators of the past decade from Microsoft to Intel, Amazon, Google, eBay, and ChoicePoint have attracted their fair share of attention and criticism, not to mention regulatory scrutiny.
Sometimes companies can get too far ahead of the curve and trigger negative public reactions, either because the activity generates negative unintended consequences, or because it is offensive, or susceptible to exaggerated public fears. Privacy concerns are often dormant until shaken by a confluence of circumstances and developments.

Indeed, it is rarely technology itself that constitutes the privacy risk but, rather, the manner in which it is used by human decision makers. For example, where some see utopian efficiencies, conveniences, and personalization in the deployment of RFID applications, others may see dystopian architectures of surveillance and control.

Consider the case of German retailer Metro, which in 2003 began an RFID trial in customer “payback” loyalty cards. Metro did not tell its customers what it was doing or why. When the RFID trial was discovered by accident, it generated a public backlash, resulting in international boycotts that continue to this day. The company’s clumsy denials and public relations handling of the incident did little to assuage privacy concerns. Although no law was broken, trust in the large retail store operator was shattered. Metro eventually recalled the loyalty cards and replaced them with non-RFID versions, but the damage was done.

Compare this experience to that of ExxonMobil who, in 1997, developed the wireless payment application known as SpeedPass. Using RFID key fobs, six million consumers have utilized the payment option at 7,500 SpeedPass-enabled locations. The technology has been a great success, enabling Exxon to increase its customer satisfaction, retention rate, and market share.

Unlike Metro, Exxon’s initiative was above-board customers enrolled for the tags, clearly giving their informed consent. Secondly, the technology provided clear and demonstrable benefits to all customers allowing fast, convenient, secure payment at the pump obviated the need to produce and use a credit or debit card.

Right now, Metro and several other global manufacturers and retailers contemplating RFID deployment are busy contending with organized worldwide consumer boycotts and considerable attention from a broad range of government and regulatory agencies, privacy advocates, and consumer interest groups.

ONE growth and success will be predicated on a virtually insatiable appetite for information. New technologies allow and even encourage the collection of evermore...
fine grained data about customers and their transactions that are then analyzed for insights and competitive advantage. What choices will firms make in the responsible use and deployment of technologies that can manipulate this data?

5.3 Digital footprints
Every time a cellphone is used, a website is visited, or a debit card swiped, a digital footprint is created. That digital footprint, pertaining to an identifiable consumer, is used by a company, or companies, to construct a profile of patterns and preferences which can then be used for promotion and marketing purposes.

These digital footprints are very valuable to marketing and advertising departments, and will become even more valuable in the future as tracking technologies improve and proliferate. Internet usage has become one of the most closely tracked activities in the last decade. It has even given birth to an entirely new industry of specialized customer tracking software.

In October 1999, an independent security analyst discovered that RealNetworks had assigned a global unique identification number (GUID) to each of its users who registered with its popular Real Jukebox software, and was using that number to track music listening patterns.

Although RealNetworks claimed that the data were only used for aggregation purposes, GUID technology potentially enabled RealNetworks to create personal profiles that included everything from listening preferences to credit card numbers. This type of data collection was in direct contradiction to RealNetworks’ stated privacy policy. The company subsequently amended its privacy statement to alert customers to the types of information that might be gathered, and released a software patch for users to block transmission of their personal information.36 Angry customers, however, initiated two lawsuits against the company.37

Since then, consumer concerns and fears regarding clandestine online surveillance and data collection have continued to grow, and trust is continuously being eroded. Digital rights management technologies, for example, track and control online media usage with fine grained precision. Similarly, spyware small software applications that surreptitiously install themselves on one’s computer to track user activities has become a problem of epidemic proportions. U.S. lawmakers are wrestling with the spyware problem through appropriate legislative responses. In an effort to gather increasingly detailed information about online customers and generate metrics for marketing initiatives, many companies routinely insert “Web

---


bugs” in their marketing email messages that report back when and how often the message was viewed, by whom, and what actions or links were followed. Very few people are aware of this now common online marketing technique; it is ripe for a privacy backlash or strong privacy self-defence techniques.

In sum, the overzealous or irresponsible deployment of invasive information and communication technologies can undermine the credibility of privacy promises and, in some instances, trigger strong consumer and legislative responses.

5.4 Possible solutions
The ONE must carefully consider the legal, public relations and economic risks of adopting any technology enabled data collection strategy.

To start, it is important to recognize that much of the information that is collected is, in fact, personal in nature, meaning that it may lead to identifiability. Even if the information itself, such as a computer IP address, software unique ID, or shopper’s card movements in a store is not personally identifiable per se, what matters is whether the data can be linked to an individual. In this context, firms should recognize and address the possibility that, if they can collect this data, others may be able to do so too. For example, an RFID tag embedded in a loyalty card could also be read by competitors.

It is important to limit collection to what is strictly necessary. Too often firms collect data simply because they can or because it has potential value.

It is very important to have clear privacy policies that are brought to the attention of the customer at the time of data collection. Firms should be very careful not to assume they know their customers’ expectations and that “implied consent” has been given. If there are residual privacy and security risks, these should be noted and addressed.

Successful companies will always offer meaningful choices and controls to consumers, and invite their participation and feedback. For example, customers should be able to disable or control features or easily decline or uninstall unwanted software. And new technological deployments may be more readily accepted by consumers if there are clear, direct and demonstrable benefits, rather than general promises of improved administrative efficiency, personalized service, better choices and special offers.

Firms should make, and keep, their privacy promises. Doing so establishes credibility and trust over time, and helps to build the customer goodwill that will be necessary in the event of a privacy breach.

Lastly, firms should have a realistic crisis-management plan. The successful ONE lives on the “bleeding edge” and must be ready for hard to quantify risks. Too often, ICTs are adopted and deployed without an adequate appreciation of the possibility of a privacy breach and the ensuing backlash.
6.0 Conclusions

The overarching theme relating to privacy in response to the Open Networked Enterprise is accountability. The successful ONE of the future may very well be global, decentralized, open, borderless, modular, flexible, empowering and so forth characteristics that seem to reflect the Internet itself but these same qualities challenge the responsible management of vast storehouses of customer information necessary for the ONE to succeed.

Remember to keep your focus on the customer. Taking a customer centric view of information will highlight the distinction between personally identifiable information versus non personal information. The difference between how firms treat each is critical.

Dr. Ann Cavoukian is Ontario’s first Information and Privacy Commissioner to be reappointed for a second term. Initially appointed in 1997, her role in overseeing the operations of the freedom of information and privacy laws in Canada’s most populous province was extended to 2009. Like the provincial auditor, she serves as an officer of the legislature, independent of the government of the day.

She is recognized as one of the leading privacy experts in the world and is frequently called upon to speak at major forums around the globe. Her published works include a book entitled Who Knows: Safeguarding Your Privacy in a Networked World (McGraw-Hill, 1997), written with Don Tapscott, and, most recently, The Privacy Payoff (McGraw-Hill Ryerson, 2002), in which she and the book’s co-author, journalist Tyler Hamilton, address how successful businesses build customer trust.

Dr. Cavoukian joined the Office of the Information and Privacy Commissioner in 1987, during its startup phase, as its first Director of Compliance. In 1990, she was appointed Assistant Commissioner. 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.
The New
Federated Privacy Impact Assessment (F-PIA):
Building Privacy and Trust-Enabled Federation

January 2009
Foreword

Throughout my career as a privacy professional and as the Information and Privacy Commissioner of Ontario, Canada, I have always advanced the view that, “privacy is good for business – good privacy is good business.” A lack of attention to privacy can have a number of adverse consequences for businesses, ranging from damage to reputation and brand to, most important, loss of customer trust and loyalty. This problem has become a significant one for organizations since consumers increasingly face the ever-growing threat of identity theft, as just one example of the potential misuses of information in online activities. This is due, in large part, to the fact that the Internet was not created to deal with individuals who intend to commit fraudulent or malicious actions. To ensure the continuation of a robust and trusted online technology ecosystem, we desperately need an ability to distinguish identity thieves from legitimate users: enter “Identity Management.”

I issued my first publication on Identity Management in 2006, on the 7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity in the Digital Age.¹ This work took the concept of an “identity layer” for the Internet (a broad conceptual framework for a universal, interoperable identity system) and focused on how privacy-enhancing features can and must be embedded into the design of a universal identity system architecture.

Since that time, the Internet has continued to evolve. “Web 2.0,” as today’s iteration of the Web is more commonly referred to, has the potential to provide convenient time-saving services, tailored to the individual user. The privacy concerns revolve around the demands for greater amounts of personal information in this “new Internet” for use by multiple parties, to authenticate a user’s identity; further, these exchanges of identity information may not always directly involve the individual. Privacy involves providing individuals with appropriate control over their personal information and ensuring that adequate safeguards are in place to protect the information.² This is where Federated Identity Management (FIM) comes

¹ Available at: www.ipc.on.ca/images/Resources/up-7laws_whitepaper.pdf
² There was a time when it was believed that the more an individual had granular control over information, the more he or she could control privacy. While this is true in theory, highly detailed and fine-grained controls over information tend to overwhelm the average user because of the complexity and frequency of choices available. Thus, the true solution may involve “appropriate” controls, as determined by the context.
into play. FIM allows consumers to simultaneously and securely sign on to the networks of more than one enterprise, for the purpose of conducting various transactions, while still maintaining their privacy.

For some time now, my staff have participated as invited experts in the Public Policy Expert Group (PPEG), the Project, working alongside other member organizations, to advance privacy-enabled technologies. Together with Joseph H. Alhadeff, Vice-President for Global Public Policy and Chief Privacy Officer at Oracle Corporation (who provided significant expertise and input on behalf of the Liberty Alliance), we saw the need for a resource to assist organizations in designing privacy into the process at an early stage, as they embarked on developing a federated system for identity management. I agreed to participate in this joint venture because I was attracted to Liberty Alliance’s holistic approach toward including privacy in the development of identity standards. In addition, its reputation for assisting organizations in establishing identity ecosystems that operate responsibly and securely, using decentralized authentication (so that a user’s personal information does not have to be centrally stored), was a real plus.

From a practical perspective, I believe that FIM holds the promise of serving as the fundamental element in creating an identity layer to which consumers can entrust their personal information. Privacy protection is not available in a standard one-size-fits-all model. Each business is unique, and privacy needs are equally unique, which is why I encourage businesses to develop a “culture of privacy.” By a culture of privacy, I mean developing a “mindset” – a way of thinking throughout the organization that is committed to better information management practices that are respectful of privacy. Even the most advanced technologies, coupled with the most rigorous privacy policies, will not be effective if they do not become an accepted part of your business culture. This white paper will assist organizations to achieve greater user trust in such a federation – an admirable goal. At its essence, it is a practical assessment of how privacy can be applied to a group of organizations and businesses that wish to create a community to manage their clients’ identity – one that is based on trust.

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner of Ontario
Canada
1 Introduction

1.1 The Web 2.0 World

Our world is becoming increasingly interconnected. Distributed networks of service and information providers are operating across global information and value chains. Observing, with greater frequency, dense inter-networking, large-scale data sharing, and the constant evolution of relationships between organizations, it becomes clear that firms are moving from “multinational” to “global” in nature, and that the concept of enterprise has morphed into the concept of an ecosystem.\(^3\) We are seeing the emergence of more than just Web 2.0 – we are, in fact, seeking out the World of 2.0.

In the online realm, new Internet services are exploiting the potential to provide detailed personalized services to individuals in every facet of their information-laden lives.\(^4\) The benefits related to these services, however, create information trails and broader possibilities for unauthorized access that require new considerations related to information protection. In these new paradigms, personally identifiable information becomes digitized, routed and processed on high-speed, high-capacity networks that are independent of each other, with fewer traditional hallmarks of information collection and control. New trust models are now being considered to deal with these information flows across distinct organizations at the ecosystem level (see our recently published white paper regarding the privacy implications of digital identity).\(^5\) Concepts such as cloud computing, in which organizations share both data and processing resources in order to coordinate a business process, are also beginning to take hold, creating new opportunities for cross-ecosystem industry collaborations.

As a first step toward creating trust in this new inter-networked or “federated” model, organizations are building secure ways in which to collect and store personal information. There are a number of technical means to ensure that information moving between organizations is securely transferred. However, technology is only part of the solution. Technology operates in support of people, policies and procedures, and in conjunction with the legal instruments that bind parties to the obligations related to the appropriate deployment of technology. As these enterprises and organizations start developing ecosystem-based rules and procedures, new tools will be needed to evaluate and oversee the deployment of technology, the implementation of policies and procedures, and the operation of contracts.

---

\(^3\) For more, see the IPC publication *Privacy and the Open Networked Enterprise*, December 2006, at: [http://www.ipc.on.ca/images/Resources/up-opennetw.pdf](http://www.ipc.on.ca/images/Resources/up-opennetw.pdf)


\(^5\) See the IPC publication *Privacy in the Clouds*, May 2008, at: [www.ipc.on.ca/images/Resources/privacyintheclouds.pdf](www.ipc.on.ca/images/Resources/privacyintheclouds.pdf)
Such tools are necessary to demonstrate that systems that may be technically sound can also be trusted by individuals. This paper looks at a number of the concepts underlying FIM, important practice considerations, and one of the most important baseline tools needed for the trust-enabled ecosystem – the “Federated Privacy Impact Assessment,” or F-PIA.

1.2 Federated Identity Management (FIM)
As we move forward from an enterprise model, where individuals interact with companies they know, to an ecosystem model, where information is shared within and across enterprises and value chains for a variety of purposes, new ways of dealing with personal information related to identity must be created. Federated Identity Management (FIM) systems are emerging to fill this gap – to create the Internet’s missing identity layer.6

Within the FIM model, identity credentials issued to a user by a particular service or institution are recognized by a broad range of other services. Though complex to implement online, this is similar in concept to, and can provide improvements over, traditional identification schemes in the “physical world.” A typical example would be government-issued ID credentials (birth certificate, driver’s licence, passport, citizenship card, etc.) issued by an institution (a government agency) that is broadly recognized by others (as proof of name, address, age, etc.). The user of the service does not need to prove his/her identity with each transaction; rather, it is enough to show that he/she has, at some prior point, been authenticated by a trusted authority. The service’s burden then lies not in identification of the presenter but in the verification of presented credentials – a much less onerous task. The improvement in the online federated model is that systems can be architected to ensure that only the least amount of relevant data needed to establish a credential is provided to a requestor. Going back to the driver’s licence example, if the licence is being used for age verification, there is also other identifying information that may be seen or scanned, which is unrelated to age. Further, most age verification requirements relate to age ranges, and thus do not require review of an exact birthdate. In such a situation, an FIM-based validation can, unlike the licence, return only a statement that the credential’s holder is over 18, 21, or 65 –

---

6 For more information on the missing layer, see the IPC publication 7 Laws of Identity: The Case for Privacy-Enabled Laws of Identity for the Digital Age, at: ipc.on.ca/images/Resources/up-7laws_whitepaper.pdf
whatever the relevant range – without revealing any additional information about the individual.\(^7\)

Situated online, Federated Identity Management has the potential to allow individuals to use the same username and password, or other personal identification, to securely sign on to the networks of more than one enterprise, in order to conduct transactions while maintaining privacy protections (a process known as “single sign-on\(^7\)). Federation can allow companies to share applications and information securely without the need to maintain full user accounts for their partners’ clients (a helpful privacy best practice). Open technology standards enabling FIM can also ensure choice and flexibility as various competing technology providers serve the marketplace, and can interoperate while not assuming that multiple companies will mirror each other’s technology choices. Readers should, however, note the use of conditional statements (“has the potential to,” “can”) in describing the ability of FIM to provide the above benefits. The ability of FIM to successfully create such conditions is founded upon the implementation of appropriate policies related to the technology in use.

Among the factors that need to be considered, and which will be discussed further in this paper are: appropriate notice, choice and control options, data minimization, least-means access\(^8\), compliance, audit and oversight. While not yet a term of art, for the purposes of this paper, we will refer to such a responsible and accountable model as a Privacy and Trust-Enabled Federation.

\(^7\) An online Federated Identity Management system that, as of late, has been gaining user share is OpenID. Rather than registering a new ID with each newly visited site (which requires a new username and password as well as the disclosure of some level of personal information), a user is allowed to create an identity with a single “provider” (such as Yahoo, AOL, Verisign, etc.). When the user logs into the newly visited site, called the “relying party,” the provider is queried for authentication of the user; at this point, the user is redirected to the website of the provider, gives his or her password (if the user is not already logged into the provider), and is asked if he or she wishes to trust the relying party website. Upon agreement, the user is logged into the relying party’s site using his or her OpenID, thus creating for the user a single sign-in experience.

By taking the storage of identity information out of the hands of individual websites, OpenID allows users a higher degree of informational self-determination. This architecture allows for the possibility that rather than being forced to disclose personal information (and understand the associated usage policies) at each site that requires a log-in for full interaction, a single, trusted (by the user) identity provider can be chosen for all authentications.

\(^8\) Least-means access is a concept that bridges or combines two essential privacy concepts, namely least-privilege access and data minimization. Least-means access, in plainer language, is a principle that the least amount of information should be provided to meet a request and that should be further evaluated based on the access privilege of the requestor. This concept helps ensure that those requesting information have appropriate privileges to request, and an actual need for, the information they are requesting to accomplish a legitimate business purpose.
Along with the user, an FIM architecture typically contains (a minimum of) the following roles:

- **Service Provider** (SP), or **Relying Party** (RP): A Web application that provides a service to the user, but which has outsourced user authentication. This service thus “relies” on a third party to provide identity information. There will be multiple Service Providers within the FIM “ecosystem.”

- **Identity Provider** (IP): A website or service with which the user has established his/her identity. The IP provides identity verification services to the Service Provider, and may also be a central store of user information, to be distributed on a least-means access basis. There may be one or more IPs in the FIM ecosystem.

- **Discovery Service**: A means of finding an Identity Provider that is acceptable to both the User and the Service Provider; this could be as simple as a drop-down menu on the SP’s website.

While all the roles outlined above are part of an FIM architecture, they do not necessarily represent different entities. In fact, one should consider that a large enterprise may span the entirety of the architecture, with different organizations within the enterprise playing the various roles. Building upon these roles, Figure 1 describes a typical series of interactions within the FIM architecture:

![Typical Transaction Sequence in the Federated Model](image_url)

**Figure 1:** Federated Identity Management transaction sequence

9. Service Provider or Relying Party examples can include: public-facing Internet websites (such as an online store, blog, or community forum) and private enterprise systems (such as networked databases, procurement and human resource systems).

10. Identity Provider examples can include: public-facing Internet sites (such as banks, Internet Service Providers, or an online store) and private enterprise systems (such as corporate or partner directories).
By way of illustration, we will consider a Federated Identity Management system with which most readers will be accustomed: the banking industry’s network of automated teller machines, or ATMs. Suppose a user has an account with Bank A (step 1 in Figure 1), but wishes to use an ATM belonging to Bank B, with which the user has no prior relationship (step 2). Once the user selects his/her desired transaction, the ATM must establish the user’s identity; this is done by querying the discovery service integrated into the ATM network, which can recognize (via the card he/she has presented) that the user wishes to use Bank A for identity verification (step 3). Using the entered PIN number as verification of identity, the user effectively “logs in” to Bank A (step 4), which will confirm him/her as the account holder (step 5).

Suppose that the user’s desired transaction is a withdrawal. Along with the log-in query, the ATM sends details of the proposed transaction to Bank A. In response, Bank A does not need to reply with detailed account information, such as name or address, the amount of funds currently being held (though this is often sent for inclusion on the user’s receipt), whether the account has associated credit cards or loans, etc.; rather, the transaction can be completed with only a yes/no response to the ATM’s inquiry (with some additional information sent for record-keeping purposes). The user is thus able to minimally disclose PII to the ATM, while completing secure (and potentially quite significant) financial transactions; this is the level of informational privacy possible within the FIM model.

2 Privacy

2.1 Essential Concepts

Information privacy relates to an individual’s ability to exercise control over the collection, use, disclosure, and retention of his or her personal information. This notion is necessarily predicated on the provision of clear notice related to what information will be collected and how it will be used and/or shared. Personal information is any information, identifying or otherwise, relating to an identifiable individual. Specific PII may include one’s name, address, telephone number, date of birth, age, marital or family status, financial status, e-mail address, etc. For example, credit cards, debit cards, social insurance/security numbers, driver’s licences, and health cards contain a great deal of sensitive personal information. Moreover, it is also important to point out that almost any information, once linked to an identifiable individual, becomes personal information, be it biographical, biological, genealogical, historical, transactional, locational, relational, computational, vocational, or reputational. Hence, the definition of “privacy” can be quite broad in scope, rendering the challenges to privacy and data protection equally broad.
2.2 Why Are Privacy and Trust Essential in FIM?

Now that we understand what is meant by information privacy, what can be said of its importance to FIM? Why, in particular, should federations strive to achieve the status of Privacy and Trust-Enabled? The answer is as simple as “necessity.” End users, for instance, may already have an established comfort level with the policies and information uses of a particular company within a federation; this comfort does not necessarily extend, however, to other members of a federation. In order to encourage utilization of other federation services, these users need to create the same ease of mind with organizations across the federation, many of which will be wholly unfamiliar to them. Similarly, in order to encourage the internal strength and growth of the federation, enterprises that participate in this information ecosystem must feel that the established policies, procedures and technological rules are respected, regardless of how large the federated ecosystem. Thus, FIM is dependent on customers and federation members being confident in the ecosystem’s ability to facilitate the migration of trust between known entities and a broader range of organizations which the customer and/or federation member has little or no experience with, but that should be similarly considered trustworthy in the context of a given Privacy and Trust-Enabled Federation.11

Privacy and trustworthiness may be more difficult to establish within a federation of multiple enterprises than within a single enterprise. In a lone enterprise, there is typically a common policy framework, technology implementation and user base; many tools exist, such as Privacy Impact Assessments, with which a company can demonstrate and delineate its data protection efforts. Across multiple enterprises, however, there will likely be many different policies, deployed technologies and types of users, all of which need to be both interoperable and consistent in the protections provided for shared data. Strong privacy measures undertaken by a single enterprise become meaningless if its data-trading partners do not have compatible measures; the policies and technologies of all federation members must satisfy the requirements of the trusting party.12

In order for a user’s trust to be maintained, individuals need to know that information about them that enters into this distributed web of systems will be handled according to established rules/frameworks and in conformance with promises made at the time of collection. For an ecosystem to be effective, rights to information must be apportioned across parties to meet legitimate needs, and users must be provided with appropriate controls related to their information. The majority of users, however, are neither capable of nor interested in micromanaging the ecosystem.

11 Note that the term “customer” is used broadly as a term that can encompass consumers, citizens and organizations.
12 An assurance that becomes easier in a least-means environment.
They will rely on their relationship with the organization that is their gateway/portal to the ecosystem, or with which they are ultimately connecting. Responsible organizations want to provide such assurances, both for building trust with individuals and for demonstrating compliance with various privacy regulatory environments.

Federated identity management presents a new challenge to privacy, in that transfers of personal information occur between organizations as well as between the individual and an organization. However, it is not the first technology to take the transfer of PII out of an individual’s hands. In 1999, the IPC, along with the Dutch Data Protection Authority, looked at the concept of intelligent software agents. Such agents require access to the personal profile of the individual whom they serve, in order to complete tasks on behalf of a user without any direct supervision. Much as is the case of FIM, considerable user utility may be derived from the automation of routine tasks in this way. The user should not, however, have to sacrifice privacy in order to gain these benefits; appropriate controls on the functioning of the agents (limiting of scope, use of trusted sources, deployment of appropriate privacy-enhancing technologies, etc.) can, in fact, turn an agent from a privacy threat to a privacy protector. The same can be true for FIM.

Beyond the conceptual framework, practical aids are required to help system architects and implementers, as well as the people who develop the business and information use models, to enable trust at the design and development stage. To that end, this paper will aim to provide guidance for designers looking to build trust into systems, and describe useful tools to evaluate the level to which trust has been enabled and facilitate oversight and compliance.

2.3 How Can Privacy Be Enhanced by FIM?
Using Federated Identity Management to create a community of trust can provide significant benefits for the end user, as well as for participating organizations and oversight authorities. For an end user, the leveraged trust model permits him or her to authenticate across various different organizations with only a limited amount of information transmitted among organizations. Enterprises using this model only share information in a “least means necessary” manner, based on what is absolutely necessary for a given transaction. End users can also be assured of greater consistency of security requirements and policy conditions among the participating enterprises. Enterprises and organizations that participate in a community of trust have a basis for offering new kinds of services through a broader range of organizations, thereby providing greater value to end users through their trusted relationship. When applied across enterprises to an ecosystem, this combination of policies, practices, and tools, supplemented by contracts (where needed), creates
an overall privacy framework for the federation. Such a framework can then be compared against existing guidelines such as Fair Information Practices (FIPs). This will be beneficial to the design of a federation in that FIPs have been codified in many jurisdictions (Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA), the OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Information, etc).

In our work promoting our idea of Privacy by Design\textsuperscript{14}, the IPC has also established a framework concept for a Global Privacy Standard (GPS) for technology development.\textsuperscript{15} The GPS is not a technical standard per se, but rather a distillation of fair information practices and privacy principles, which are common to many of today’s legal frameworks related to privacy and data protection. While the principles of the GPS do not represent a globally accepted norm, they serve as an effective preliminary guide to the introduction of important legal concepts and a “culture of privacy” into a federation. Below is a discussion of these principles, along with the practical ramifications for a Privacy and Trust-Enabled Federation member.

2.3.1 Consent

In a majority of legal systems that have addressed privacy, the individual’s free and specific consent is required for the collection, use, or disclosure of personal (or sensitive) information, except where otherwise permitted by law. The “quality” of this consent is context dependent; clearer and more specific consent will likely be required as the sensitivity of the data rises. Consent is also not permanent, and may be withdrawn or revoked at a later date.

The “circle of trust” created by a Privacy and Trust-Enabled Federation allows member enterprises the possibility of collection and disclosure via the notion of “implied consent.” This means that if the user is aware that services are being provided by a federation (i.e., clear and direct notice is given to the user), and not necessarily a single enterprise, then information can be shared for the purposes specified at the time of collection between trusted federation members, without the requirement of explicit user consent at each disclosure. This principle has been applied, for instance, in Ontario’s Personal Health Information Protection Act (PHIPA), which notes that health information custodians are permitted to assume implied consent (within the circle of care) to “collect, use, or disclose the information for the purposes of providing health care or assisting in providing health care to the individual,” unless it is known that consent for such has been explicitly withdrawn.

\textsuperscript{14} “Privacy by Design” is a term coined in the ’90s by the Ontario Information and Privacy Commissioner, Dr. Ann Cavoukian, in an effort to enlist the support of technology to protect privacy, rather than encroach upon it. By embedding privacy into the design of various technologies, and actually building it into the architecture of the technology involved, privacy is far more likely to be protected, instead of being viewed as an afterthought.

\textsuperscript{15} See Appendix 1 for the complete Global Privacy Standard.
2.3.2 Specified Purposes
As a second principle, organizations should specify the purposes for which per-
sonal information is collected, used, retained, and disclosed, and provide notice
to the data subject at or before the time of collection.¹⁶ The specified purposes
should be clear, limited and relevant to the circumstances.

2.3.3 Collection Limitation
Personal information should not be collected for collection’s sake; rather, collec-
tion should be fair, lawful, and limited to that which is necessary for, and consis-
tent with, the purposes specified to the data subject. As such, organizations should
uphold the principle of data minimization, meaning that collection of personal data
should be kept to a minimum. In addition, the design of programs, information
technologies, and systems should begin with non-identifiable interactions and
transactions as the default settings, and wherever possible, identifiability, observ-
ability, and linkability of personal information should be minimized.¹⁷

2.3.4 Use, Retention, and Disclosure Limitation
The use, retention, and disclosure of personal information should also be limited to
the purposes identified to the individual, except where otherwise required by law.
In addition to such a limitation, organizations within a Privacy and Trust-Enabled
Federation should use and disclose data in a least-means access manner; that is,
only the minimal data necessary (e.g., an age range, instead of an exact birthdate)
for a specific transaction should be made accessible – this applies to both trans-
fers of data between enterprise members and within the data-holding organization.
Organizations should also retain personal information only as long as necessary to
fulfill the stated purposes, after which time it should be securely destroyed.

2.3.5 Accuracy/Access
Neither organizations nor individuals should be satisfied with the use of inaccurate
data within an enterprise or a federated ecosystem. In addition to the negative im-
pacts on business, incomplete, out-of-date, or inaccurate data can have significant
bearing on individuals, particularly in the case of qualifications required to access
services in a federated ecosystem.

---

¹⁶ In some cases, information is collected as part of the technology handshake between systems – so
things like the IP address of a computer and other related information may be captured before a no-
tice of purpose may be provided. Some principles can thus be modified with the term “or as soon
thereafter as practicable” to account for these automated collections related to system functionality.

¹⁷ There are, of course, transaction requirements that require identification from both a legal and busi-
ess perspective; tax reporting, delivery requirements etc. We recall, however, the driver’s licence
example and highlight that even where identifiable information needs to be collected, concepts of
data minimization should be applied.
As a principle, then, organizations should ensure, with varying degrees of exactitude depending on the context, that personal information is as accurate, up-to-date and complete as required for the specified purpose.\(^{18}\)

In addition to organization-initiated data integrity checks, the issue of data accuracy can be addressed by the adoption of another privacy principle: access. This principle states that individuals should be provided with access to data collected about them, along with information about how that data is being/has been used and/or disclosed. Further, individuals should be provided a challenge mechanism, to address any perceived inaccuracies or deficiencies in the data. Allowing user access thus not only addresses a commonly held privacy standard, but it also brings the individual – in theory, one of the ultimate authorities regarding his or her personal information – into the solution of ensuring data accuracy.\(^{19}\)

### 2.3.6 Security and Data Integrity

Organizations must assume responsibility for the security of personal information throughout its life cycle consistent with the international standards that have been developed by recognized standards development organizations. Personal information should be protected by reasonable safeguards, appropriate to the sensitivity of the information (including physical, technical and administrative means).

### 2.3.7 Accountability/Openness/Compliance

Finally, the collection of personal information entails a duty of care for its protection. Obligations related to all relevant privacy-related policies and procedures should be documented and communicated as appropriate, and assigned to a specified individual within an organization. When transferring personal information to third parties, organizations should seek equivalent privacy protection through contractual or other means. Further, in order to ensure the accountability of federation members, the principles of openness and transparency should be adopted. That is to say, information about the policies and practices relating to the management of personal information should be made readily available to the individuals whose data is being held.

Organizations should also establish compliance and redress mechanisms, and communicate information about them to the public, including how to access the next level of appeal. Compliance with privacy policies and procedures should be monitored, evaluated, and verified on an ongoing basis.

---

\(^{18}\) There is a complexity here, in that both access and accuracy can be difficult, if not impossible, to maintain down the chain of data custody. Such custodians must, however, ensure data security.

\(^{19}\) A number of enterprises have also found that self-service registration and maintenance of such information by the user not only increases accuracy, but also decreases the costs of operating and maintaining both the systems and the support functions.
The combination of these factors leads to the concept of accountability, in which information is appropriately secured and protected across both the scope of federated enterprises and the life cycle of the information. This concept not only forms the basis of Canadian privacy laws, but is found in the OECD Guidelines, and is the defining principle of the APEC Privacy Framework.

2.4 Role of Fair Information Practices and Global Privacy Frameworks

Frameworks such as GPS and Fair Information Practices are not, of course, intended to supersede legislation – an issue that must be considered within a federation, given the likely trans-border nature of data flows. Instead, such documents should be considered as guidance which can inform federations and federation members about essential privacy concepts, regardless of jurisdiction.

3 Risk Assessment

To effectively examine an information ecosystem, one must be familiar with the life cycle of the data contained therein. Information is collected, shared/used, refreshed, or deleted, for a variety of purposes. The cyclical nature of the information life cycle must be supported by appropriate policies, practices, procedures, tools, and contracts. While the categories and principles of the life cycle are fairly constant, how they work, for what purposes they are used, and how they are supported varies from company to company, and ecosystem to ecosystem. These are dependent on the needs, types of information, sensitivity of information, policy choices and a number of their variables. Evaluating such life cycle considerations presumes a familiarity not only with the needs of the entities involved but also with the risks that those entities may face.

Thus, a foundational element of the Global Privacy Framework is a proper threat risk analysis. Risk must be properly identified, minimized to the extent possible, and appropriately managed where it can’t be eliminated. Recall that risks come in a broad range. Many considerations of risk are based on concepts of traditional compromise of systems – i.e., breach by an outsider. There are also risks that are harder to identify and control, arising from insider threats. Other risks include the potential for operational failure: from massive system failures to issues like failing

---

to anonymize information sufficiently to prevent identification. These risks could be a matter of degree, or an issue of implementation/deployment.

A large part of appropriate risk mitigation and management is proper training, preparation, and incident response. No single system or ecosystem is foolproof, so training, preparation, and response are essential concepts because incidents invariably occur. A proper contemplation of the information life cycle includes these concepts. An entity that has taken the right preparatory steps will debrief incidents to see where improvements can be made, thus becoming a learning organization. In more advanced learning organizations, tests of processes and procedures related to incident response can provide much of the valuable learning, prior to an actual incident arising.

4 Federated Privacy Impact Assessment

For some time now, organizations with privacy compliance programs to protect privacy and the confidentiality of personal information collected use a tool known as a Privacy Impact Assessment (PIA). The PIA is one of many tools used to assist organizations to ensure that the choices made in the design of a system or process meet the privacy needs of that system, typically by way of a directed set of questions, based on privacy requirements. In some circumstances, it may be conducted alongside a threat/risk assessment, which is one of the inputs into assessing the overall privacy landscape. A PIA can be applied for the purpose of a systems requirement definition to a single project, or for the purpose of demonstrating regulatory compliance to an enterprise. A PIA must be considered in the context of the needs of the organization, the uses of the information, and the relevant fair information practices that are either required by regulation or otherwise adopted by the organization.

All PIAs should have a modular nature since most policies, governance frameworks, and systems are neither the purview nor expertise of a single person. A PIA will have a coordinator or point person within an organization, often the Chief Privacy Officer (CPO). The CPO should assemble the organizational team required to review

“A privacy risk assessment should become an integral part of the design stage of any initiative. Once the risk to privacy is identified, then the necessary protections can be built in to minimize or ideally eliminate the risks.”

All PIAs should have a modular nature since most policies, governance frameworks, and systems are neither the purview nor expertise of a single person. A PIA will have a coordinator or point person within an organization, often the Chief Privacy Officer (CPO). The CPO should assemble the organizational team required to review

21 Organizations may develop polices and practices that interpret legal requirements; at times these policies and practices may exceed legal requirements, including where there are global practices that are in place despite the lack of any local regulatory or legislative requirements.

and answer the PIA questions. In a corporate setting, that team would include representatives from technical support/customer service, security, marketing, and relevant lines of business. Optimally, the various owners/operators of the systems and other framework elements will have been consulted in the development of the PIA, and the PIA process will yield benefits to them as well. The PIA has two roles: one is assisting in privacy compliance, but the other, which has greater meaning for participants not responsible for privacy, is to be a building block of the information governance and risk management program of the company. The identification of the PIA in this manner will assist those disciplines not specifically concerned with privacy to better understand both the value of the review, its relevance to their job function, and the role it plays in adding value to the organization.

When organizations come together in a federated ecosystem, a new conceptual application of the PIA is required: the Federated Privacy Impact Assessment (F-PIA). The F-PIA differs from a traditional PIA in a number of ways. Most importantly, the F-PIA is designed to operate either within an enterprise (such as one where a number of different systems may be federated together) or across enterprises that have different needs and uses of information. An F-PIA must be designed to accommodate various starting points, from situations where most systems have already gone through some form of a PIA (in which case a focused gap analysis will be an effective starting point for the F-PIA), to more “green fields” settings where most of the systems requiring review have not undergone a PIA (in which case an F-PIA at the level of the federation can act as a template for initiating organization-level PIAs). While major elements of the F-PIA will seem familiar, they are designed to be applied in a more flexible fashion.

An F-PIA is designed to consider data “in motion” (that is, being transferred among various organizations), rather than data “at rest” (which is more relevant to a traditional PIA). The question of the exchange of information within an identity federation is in some ways more simple, and in some ways more complex, than questions asked in traditional PIAs completed by an organization. Simplicity can be found in that the nature of an identity federation will typically mean that the personal information that is involved in the federation is well specified and that data flows are documented. Each member of the federation has a defined role, or roles, such as Identity Provider (IP), Service Provider (SP), and Discovery Service (DS), and so on.23 The type of personal information each role is entitled to should be well defined as part of the technical specifications of the federation. This fact by itself bypasses some of the most onerous aspects of a PIA within an organization, especially one with substantial amounts of unstructured data or data in legacy applications.

23 It is important to note that an organization may play more than one role in a federated ecosystem. As time and experience with these ecosystems progress, this merging of roles is becoming more commonplace.
There is, however, complexity in an F-PIA that does not exist in an organizational PIA. As the subject of an F-PIA is "data in motion," it will, in some cases, mean that data will be passing between regulatory jurisdictions, between different industries, or across borders (PIAs should also take this consideration into account in the case of multinational corporations or the off-shore outsourcing of data). Thus, questions of technical accountability and custody of personal information arise that are not present in the single organization context. In many regulatory regimes, you may be able to outsource services, but you cannot outsource accountability. This means that every organization involved in a federation is a stakeholder, even if a particular data flow is not one in which it participates.

The F-PIA is also meant to be reusable. Due to the non-static nature of federations, it would be impractical to perform an ecosystem-wide privacy assessment for each added member or service. Such an undertaking is not expected. Instead, a new addition to a federation should be able to identify the role (or roles) that it will play, along with its corresponding responsibilities and requirements. In each of the models that follow, the opportunity exists to create, through an F-PIA, a set of privacy- and trust-enabling standards against which additions to the federation can be compared.

### 4.1 Nature of Federation

When an identity federation forms, establishes, or applies a set of privacy standards to be observed for the purposes of the federation, and elects to conduct an F-PIA, it will be faced with the question of how to coordinate the privacy policies, procedures, and practices of its disparate members. Federation can take a number of forms, ranging from a fluid and changing set of equal partners to a centralized group of subsidiaries, under the direction of a central body. The structure of the federation will establish where the authority to determine the privacy standards for that federation lies, subject to overriding legal constraints. The nature of federation will also aid those who undertake an F-PIA to determine the likely source of threats to such standards.

#### 4.1.1 Collaborative Model

In the collaborative model, a group of founding members or member forms an entity that establishes the rules for the operation and governance of the ecosystem, as well as overseeing day-to-day control of the system. Described as the most complex of the models of federation, but with the greatest flexibility, this model is paradoxically likely to require the most rigid privacy rules and stringent F-PIA. These
controls are put in place to ensure that the indefinite membership and flexibility may not be exploited to extract PII for inappropriate uses. Assurances of minimum disclosure and strict technical enforcement of privacy guidelines will require audits and accurate user reporting to engender appropriate trust in verifiable privacy. The Governing Entity in the model will be the central authority for privacy compliance.

4.1.2 Consortium Model

In the second model, a small number of founders forms a consortium via a multi-party contract that sets the rules and governance for the ecosystem. Based on reasonably autonomous founders, the risk to privacy in the consortium model is that one or more of the founders may have a significantly different privacy model. With respect to the exchange of PII, the contractual agreement by which the federation is formed must be specific as to the common privacy elements. The F-PIA created for such a federation will need to be clear on the limits of the assertions that can be made for the consortium. It is very likely that the privacy assertions of the whole federation will be the “lowest common denominator” of the founders. Where consortiums develop from a common industry with a common expectation of practice, this may not present a significant bar, but in cross-industry consortia, this could generate friction.

4.1.3 Centralized Model

In the centralized model, a single founder sets the rules and governance for the ecosystem, and contracts individually with each other member. This approach provides the founder with a significant amount of control, and significantly less control to the other members. The centralized model ensures that data flows through,
or with the awareness of, the single founder, which implies that privacy assertions can be made and verified by that organization. This architecture also allows for the possibility of the single founder incorporating the data protections identified and afforded by the F-PIA to be contractually incorporated into the federation, in a highly uniform manner.

4.1.4 Service-Oriented Architecture

While complexity is increased in a service-oriented architecture (SOA), the analysis and impact assessment may actually be simplified. A useful way to think about an SOA is as a cloud of service elements that can be associated in a number of ways, either dynamically or in a directed fashion, to provide a service. The complexity is created by the potential for differing service elements to be joined together to create various desired solutions. In order to prove these results at a later time, there may need to be a record of the elements used in a given solution, as well as the characteristics of the elements since they may change periodically. In an F-PIA, an analysis related to an SOA architecture may be simplified by using the same modular approach. Taking cues from the design principles of SOA, F-PIAs can be assembled in a modular and reusable fashion as well by evaluating the various distinct modules and reusing the information gathered in an overall privacy evaluation of the inputs and ends of the service chain – the information that is accessed by the service, and the output of the service element used. The SOA environment should be evaluated on four parameters: security of the elements, auditability of elements, access control and system oversight/accountability. Once the elements have been evaluated, they can be reused in combination with greater confidence and lower overhead.

Regardless of the architectural model or legal form, in most cases, it is likely that there will be a mixed level of privacy practice across the federation. Some members, in particular, may have access to less, or less sensitive, personal data, and thus may need less elaborate protections and compliance procedures to provide appropriate safeguards. While there may be some temptation, for ease of implementation or for simplicity’s sake, to “race to the bottom” and for the federation to adopt the “lowest” privacy standard of any of its members, this is likely to be counterproductive in the long run. This is particularly true if privacy is to be a source of competitive advantage
or the basis of trust between federating entities and their end users (citizens, consumers, and employees). Instead, member organizations must always ensure that they deploy data protections commensurate with the risks they face.

5 F-PIA Goals and Value Propositions

5.1 Data Subjects and Regulators
Besides the organization(s) involved in the federation, a number of other stakeholders exist who do not directly participate in the F-PIA, but who may utilize the results or rely on its process to safeguard their interests. Among the most important of these stakeholders are the data subjects, whether they be citizens, consumers, employees, or other individuals whose information is collected, processed, stored and shared by systems. Data subjects are beneficiaries of an F-PIA process to the extent that it appropriately ensures the security of the information and the implementation of related policies and procedures. Data subjects will be equally concerned that any promises made by entities within a federation are honoured and that appropriate complaint and recourse mechanisms exist.

Another major group of outside stakeholders is comprised of oversight and regulatory authorities. These stakeholders may include traditional privacy and information commissioners, relevant agencies responsible for oversight related to the protection of personal information, and private sector bodies that may be involved in trust oversight or evaluation. The F-PIA must consider a flexible way to address the needs of these stakeholders. PIAs, by their nature, may include secret and proprietary information that may not be appropriate to share in public documents. As such, the F-PIA process must consider ways to provide meaningful information related to the review without compromising either secret or proprietary information, or the kind of information related to configuration, which could be used to compromise systems security.

In this sense, the F-PIA must be considered in two parts. The first part is that which is relevant to the organizations involved and their compliance functions; the second part is a summary or redacted version of the first, which may need to be provided to oversight organizations or, where appropriate, made available to the public. The reduced information made accessible as an outcome of an F-PIA should not be viewed as a method of hiding deficiencies, but rather an opportunity to ensure that information that could compromise security, or should otherwise be protected by the organization, is not released. Under appropriate conditions, of course, oversight authorities may be able to request or require the production of more detailed information to meet their legal obligations.
5.2 What are the Goals of an F-PIA?
There are four primary goals to be achieved through an F-PIA.

**Goal 1: To provide an opportunity for members to discuss, develop, and codify a federation’s privacy policies.**
First, it is recognized that privacy policies will vary by federation. These policies should address fair information practices as appropriate to the contextual application of the federated ecosystem and the regulatory requirements to which it may be subject. In addition, the policies should recognize that the person whose data is being processed should be provided with appropriate choice and control over both who has access to, and what can and cannot be done with, their data (with allowances being made for overriding factors such as court orders or medical emergencies). However, regardless of particular policy choices, individuals must be convinced of the veracity of a federation’s claims of data protection in order to create a trusting relationship. Thus, the second goal of an F-PIA:

**Goal 2: To demonstrate that privacy policies, as defined by the members of the Federation, will be met.**
Most privacy policies require some degree of data minimization and enable legal requirements of choice or consent. Thus, an F-PIA of a system that undertakes consent-based collection of personally identifiable information must ensure that consent is properly addressed, as either open-ended or specific, opt-in or opt-out, depending on the requirements. An F-PIA evaluation of a data-minimizing policy would likewise require that only the minimum possible personally identifiable information is collected. An F-PIA would use similar analysis frameworks to address all covered elements of the policies and legal requirements, such as determining the extent to which data is shared, the uses to which it is put, and the length of time that it is retained.

Effective privacy protection, however, requires a number of system design elements to be in place, irrespective of the particular privacy standards that are applied to a system. Without a doubt, up-to-date, robust security mechanisms must be in place to ensure that access to data can be reliably restricted to only those who have an established right to the data, as established by privacy policies. Thus, the third goal of an F-PIA:

**Goal 3: To demonstrate that an appropriate technological architecture is in place to prevent, to the extent possible, accidental or malicious violations of privacy policies.**
One must recall that security does not equal privacy; security is critical to privacy, but it is a contributory factor. To perform this function, single demonstrations of technological privacy protections and security measures are not sufficient. An F-PIA should be an iterative and ongoing process. Privacy is not a momentary commitment, nor should an F-PIA be a “box ticking exercise.” It is an ongoing
The New Federated Privacy Impact Assessment (F-PIA)

obligation to actively meet the needs of organizations, promises made to individuals, and regulatory requirements. It behooves the federation to create a goal of the highest achievable privacy standards, and to revisit this goal on a regular basis. An F-PIA should be conducted for any new system or program, as well as at the point of any substantial change to systems or programs handling PII. Since an identity federation exchanges identity-related information, any substantial change in the federation or its data flows should also be accompanied by a revisiting of the F-PIA, as should any major privacy breach. The F-PIA is a living document, a tool always to have at hand either for use or revision.

Ensuring that F-PIAs are completed with appropriate candour and resources brings us to the fourth goal of an F-PIA:

Goal 4: An F-PIA should benefit all parties who complete, use, and rely on an F-PIA.

In this paper, we explored various stakeholder interests in an F-PIA. Many people who design PIAs focus only on the ultimate regulatory object of the PIA process without considering the value it can and should return to those completing the PIA. This is an especially important concept in an F-PIA, where a top-down directive within an organization is not the main motivating factor. The question for the F-PIA architect is, how to make sure that the questions and format provide useful information about a system to the designers and users of the system beyond its ability to comply with stated requirements. Often the benefits are the clarification of objectives and obligations, as well as the interaction between technology and policy across the system. Thus, architects should be aware that some aspects of the results of the F-PIA may need to be shared across entities to enable them to better understand the systems design and interrelation.

Ultimately, though, it is individual consumers who benefit most from this process, through the privacy protections afforded them. This benefit then trickles down to all federation members through competitive advantage, increased consumer confidence, and broadened consumer usage of federation services.

5.3 F-PIA Framework

Once the privacy requirements have been established, and prior PIAs have been integrated, the F-PIA becomes a matter of conducting an assessment across the entities in a federation. This is another iterative process, where strategic steps are iterated at finer levels of granularity as the F-PIA winds its way from high-level objectives to concrete determinations at the level of data and individual procedures. The key structural elements of a functioning F-PIA are the data itself, policies and procedures, technology and systems, and accountability. By creating an assessment based on appropriate fair information practices (e.g., Global Privacy Standard) that accounts and reports on these elements, an identity federation will be capable of providing assurance to all stakeholders regarding privacy-related issues.
6 Questions You Should Be Asking

The elements that need be examined in an F-PIA can roughly be divided into the following three categories: the Information Life Cycle, Organizational Principles, and Implementation. In this final section, sample areas of inquiry will be given for each. Please note, though, that the following questions are not meant to be comprehensive, nor necessary for inclusion in the F-PIA. Rather, they are presented as a means of suggesting the types of questions that should be asked in regards to privacy and security standards within a federation.

6.1 Information Life Cycle

We previously stated that it is important to create a “culture of privacy” within an organization, in order to create a trusting relationship with users. The questions asked regarding the Information Life Cycle attempt to examine this culture. In particular, a federation should consider its treatment of personal information, whether it is collected for necessary purposes, and whether its dissemination is ultimately decided upon by the individual involved – that is, the federation should contrast its practices with those prescribed by generally accepted privacy standards. Areas that should be explored within this topic may include:

1. **Appropriate Notice** – Is the individual whose personal information is being transferred aware of the transfer?
2. **Appropriate Specification** – Are the federated parties appropriately aware of the limitations related to the collection, use, sharing, and retention of information?
3. **Appropriate Consent** – Can transfers of personal information be appropriately linked to a user’s consent or choice?
4. **Appropriate Control** – Does the user have appropriate control over the transfer of his or her personal information?
5. **Data Minimization** – Do federation members collect the minimum amount of personal information necessary?
6. **Least-Means Access** – Do federation members transfer/access only the personal information needed to complete a particular transaction?
7. **Compliance, Audit and Oversight** – Is there an oversight body, or auditing or compliance mechanism, to ensure that privacy policies are met?
8. **Reporting** – Is there sufficient documentation of policies and procedures to help demonstrate compliance?
6.2 Operational Principles

An examination of the operational principles of the federation should fully describe the philosophy of interactions both among federation members, and when communicating with persons collecting data from them. Here, a focus on clarity is required: it must be shown that each member understands what is required of it within the federation. It is at this level, in particular, that the true complexities of federation may arise.

Questions provided for guidance in examining operational procedures include:

1. **Structure/Role Assignment** – Are the roles of all federation members clearly understood and transparently defined? Do federation members know their responsibilities and obligations?

2. **User Understanding** – Are the names or types of members of the federation and their roles made clear to the user?

3. **Identity Management at the Ecosystem Level** – Do Service Providers have the capacity to link a user’s profile across services, in the absence of user authorization? This may be the case if a Service Provider serves a dual role as the Identity Provider. [This topic goes to the ability of federated identity formats to enable appropriate sharing limitations.]

4. **User Involvement** – How does the federation protect against account linking, traffic and analysis? How does the federation encourage user involvement in defining controls?

5. **Worst Case Scenario** – Has a “disaster” scenario been considered, including steps to be taken to notify users and minimize any damage that may have resulted?

6.3 Implementation

An F-PIA should consider the various elements of the technical implementation of the Federation. Beginning with the design and architecture of the system, an F-PIA should include undertaking an assessment of the flows of information and how the technology is configured to ensure the privacy goals of the community of trust, or what we are calling federation. Drawing from the OECD Security principles and Liberty Alliance’s best security practices, the following framework might be followed when developing detailed questions in this area:
1 **Awareness** – Are federation members aware of the need for information and network security, and the steps they can take to enhance security?

2 **Accountability** – Are federation members accountable for information security, to the extent appropriate to their role?

3 **Response** – Is there a response action plan in place, so that federation members can co-operatively prevent, detect, and respond to security incidents?

4 **Ethics** – Do participants understand that their own action or inaction may harm other federation members?

5 **Risk Assessment** – Have all federation members individually, and at the level of federation, completed risk assessment and minimization processes?

6 **Security Design and Implementation** – Is security designed as an essential element of the information systems?

7 **Security Management** – Does the federation have a comprehensive approach to security management?

8 **Reassessment/Learning** – Do the federation and its members have a schedule for reassessing security measures and making modifications as appropriate, including reassessment after incidents or operational failures?

In addition to inter-federation security measures, technical questions regarding common security threats at the user-federation member transaction level must be addressed. These threats may involve denial of service, message replay, spoofing, brute force, or many other common forms of online attack. Sample questions that a federation, and its individual members, may wish to ask include:

1 Are user interactions (beyond the log-in process itself) authenticated? If not, what alternative measure is used to prevent session hijacking?

2 Will session tokens be used? If so, what measures are in place to prevent message replay?

3 Have authentication measures been evaluated to ensure that they are appropriate to the nature and sensitivity of the information?

Again, these questions are not meant to be comprehensive, but instead are meant to provide examples of issues that must be addressed when analyzing privacy and security measures within a federation.

---

25 Often couched as a democracy principle when applied by government organizations, all F-PIAs should have an objective ensuring that the security of information and networks is compatible with the essential values of a free society (such as free exchange of ideas, openness, transparency).
7 Next Steps

One of the concepts that the Information and Privacy Commissioner of Ontario originated and has been a leading voice for is Privacy by Design – advancing the concept of building privacy directly into technology, as part of the design and deployment process. This office strongly believes that there are great potential benefits for both consumers and organizations in the deployment of Federated Identity Management; however, these benefits can only be fully realized in the context of a Privacy and Trust-Enabled Federation. We also believe that one of the most important and effective tools for demonstrating the adoption of Privacy by Design is the Federated Privacy Impact Assessment (F-PIA).

Having examined the above material, what would be the next step for a federation? It would be the development of a formal F-PIA. This paper is only intended to serve as a guide – organizations and federations must use it, along with the numerous PIA development tools currently in existence, to create measurable standards against which privacy and trust measures can be compared. Ultimately, one must remember that in this process, a zero-sum game is not at play – functionality does not need to be traded off for privacy. Rather, building in privacy and trust in a positive-sum manner creates a win-win scenario, in which both consumer and supplier are the beneficiaries of a robust information ecosystem. Unnecessary trade-offs should become a thing of the past.
Appendix 1: Global Privacy Standard

1 **Consent**: The individual’s free and specific consent is required for the collection, use or disclosure of personal information, except where otherwise permitted by law. The greater the sensitivity of the data, the clearer and more specific should the quality of the consent required. Consent may be withdrawn at a later date.

2 **Accountability**: Collection of personal information entails a duty of care for its protection. Responsibility for all privacy-related policies and procedures shall be documented and communicated as appropriate, and assigned to a specified individual within the organization. When transferring personal information to third parties, organizations shall seek equivalent privacy protection through contractual or other means.

3 **Purposes**: An organization shall specify the purposes for which personal information is collected, used, retained, and disclosed, and communicate these purposes to the individual at or before the time the information is collected. Specified purposes should be clear, limited and relevant to the circumstances.

4 **Collection Limitation**: The collection of personal information must be fair, lawful and limited to that which is necessary for the specified purposes.

   **Data Minimization** – The collection of personal information should be kept to a strict minimum. The design of programs, information technologies, and systems should begin with non-identifiable interactions and transactions as the default. Wherever possible, identifiability, observability, and linkability of personal information should be minimized.

5 **Use, Retention, and Disclosure Limitation**: Organizations shall limit the use, retention, and disclosure of personal information to the relevant purposes identified to the individual, except where otherwise required by law. Personal information shall be retained only as long as necessary to fulfill the stated purposes, and then securely destroyed.

6 **Accuracy**: Organizations shall ensure that personal information is as accurate, complete, and up-to-date as is necessary to fulfill the specified purposes.

7 **Security**: Organizations must assume responsibility for the security of personal information throughout its life cycle, consistent with the international standards that have been developed by recognized standards development organizations. Personal information shall be protected by reasonable safeguards, appropriate to the sensitivity of the information (including physical, technical, and administrative means).
8 **Openness**: Openness and transparency are key to accountability. Information about the policies and practices relating to the management of personal information shall be made readily available to individuals.

9 **Access**: Individuals shall be provided access to their personal information and informed of its uses and disclosures. Individuals shall be able to challenge the accuracy and completeness of the information and have it amended, as appropriate.

10 **Compliance**: Organizations must establish complaint and redress mechanisms, and communicate information about them to the public, including how to access the next level of appeal. Organizations shall take the necessary steps to monitor, evaluate, and verify compliance with their privacy policies and procedures.

Please see *Creation of a Global Privacy Standard* at:

http://www.ipc.on.ca/index.asp?navid=46&fid1=575
References

Online Privacy
7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity for the Digital Age (October 2006) at:
http://www.ipc.on.ca/index.asp?navid=46&fid1=471

Creation of a Global Privacy Standard (November 2006) at:
http://www.ipc.on.ca/index.asp?navid=46&fid1=575


Privacy and the Open Networked Enterprise (December 2006) at:
http://www.ipc.on.ca/index.asp?navid=46&fid1=576

Privacy and Security
A View from 2018: A Glimpse of the Internet Future (June 2008) at:

http://www.ipc.on.ca/index.asp?navid=46&fid1=316

Privacy and Security Best Practices (version 2.0, November 2003) at:
http://www.projectliberty.org/liberty/strategic_initiatives/privacy_trust_security


Risk Assessment
Information Security Risk Assessment (August 1999) at:

INFOSEC Assessment Methodology at:
http://www.fountainheadcollege.edu/ia/NSA/IAM.htm

INFOSEC Evaluation Methodology at:
http://www.fountainheadcollege.edu/ia/NSA/IEM.htm

Risk Management Framework (August 2008) at:
http://csrc.nist.gov/groups/SMA/FISMA/framework.html

Threat and Risk Assessment Working Guide (November 2005) at:
Online Privacy:
Make Youth Awareness and Education a Priority

March 2009
Online Privacy: Make Youth Awareness and Education a Priority

For young people today, going online to connect and interact with others is a natural and integral part of daily life. As they log on to e-mail, blog, chat, or participate in online social networks, young people no longer see the Internet as simply a tool, but rather as an extension of their social lives and public identities.

While most cyber experiences are extremely positive, many young people appear to go on “auto-pilot” when they are online, not thinking twice about broadcasting intimate details about themselves on various websites. Regrettably, this has resulted in abuses and unanticipated consequences ranging from cyberbullying, identity theft, and stalking, to school expulsions and future job prospects being ruined by indiscretions posted online.

While many young people are aware of the possibility of physical threats arising from Internet activities, such as those posed by cyber predators, few fully understand the range of additional risks associated with posting too much personal information online. Most are not conscious that information can remain in cyberspace virtually forever, and can be viewed, copied and downloaded by millions of people. As a result, the personal details they share today can be used to embarrass, hurt, or stigmatize them at a later date. Similarly, their online activities can be used covertly for marketing or commercial purposes.

The Office of the Information and Privacy Commissioner of Ontario (IPC) is mandated to build public awareness about Ontario’s access to information and privacy laws. Since 2006, when social networking sites first began making headlines as a technological and social phenomenon, the IPC has made it a priority to educate the public, stakeholders, operators of websites, and especially young people about their shared responsibility to protect personal information online.

The focus of our message to young people has been that they need to be proactive and to think before they post. Nothing is ever deleted from the Internet. So we’ve encouraged them to consider that the “7 Ps” (Parents, Police, Predators, Professors, Prospective Employers, Peers, and Pals) can view their postings online and to think about whether they are comfortable with the information they are sharing. We teach them that privacy is about freedom of choice and that they can control how much personal information they post online and who is granted access to it.

We’ve used a variety of channels to reach out to youth. These include school programs, media, conferences, and partnerships with organizations that work closely
with young people. We’ve also participated in helping to form an innovative peer-to-peer network to build awareness among youth.

At the same time, we’ve also worked closely with key stakeholders, like Facebook and MySpace executives, who have the capacity to make privacy-enhancing options available to users and to spread the word about using those options to make choices about how much personal information to share online and with whom.

The IPC is part of a global community of Privacy Commissioners and Data Protection Authorities that are drawing attention to the pressing need to engage young people in managing the risks associated with their online activities. With our international counterparts, we’ve been gathering momentum behind this issue, from all parts of the world.

As we look ahead to further opportunities to enhance awareness about the privacy challenges that youth face on the Internet, it is useful to reflect back on our achievements to date, and to explore how the various channels used have contributed to supporting our educational goals.

## Engaging Social Networking Websites

### Facebook

In 2005, as Facebook was preparing to open its website to the general public, senior executives approached the IPC seeking our input on their privacy measures. We recognized immediately that collaborating with Facebook was a great opportunity to improve the range of privacy controls available to users and to increase awareness about exercising those options.

Since Facebook was still relatively new to the Internet, our first step was to develop a better understanding of the perspective of Facebook’s core users — students and youth. In August 2006, the IPC convened a focus group of 18 university students from Ryerson University, Queen’s University, the University of British Columbia, George Brown College, the University of Toronto, and York University, to discuss online social networking.

The group’s feedback was illuminating. Almost all of the students were active users of Facebook and strongly favoured it. Most were completely unaware of any potential privacy issues, had not read the website’s privacy policies, and did not know anything about the privacy filters available for their use. It was clear that more education in this area was urgently required.
Since then, Facebook and other social networking websites have exploded in popularity and are obviously here to stay. More than ever, it is critical to build awareness among young people about the importance of exercising good judgment when using social networking websites. To address this need, the IPC produced several resources aimed specifically at Facebook users:

- In October 2006, the IPC and Facebook released a joint brochure, *When Online Gets Out of Line: Privacy – Make an Informed Online Choice*, which encourages university, college, and high school students to carefully consider their privacy options before posting their personal information online.

- In May 2007, the IPC released *How to Protect Your Privacy on Facebook*, a tip sheet that outlines detailed steps on how to set privacy settings on Facebook to the optimal level of protection. The tip sheet was updated in 2009.

- In October 2007, the IPC produced another tip sheet, *Reference Check: Is Your Boss Watching? Privacy and Your Facebook Profile*, which warns Facebook users that information they post on their profile can be searched by current and prospective employers.

- In July 2008, Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario, and Chris Kelly, Chief Privacy Officer of Facebook, produced a DVD, *Be a Player: Take Control of Your Privacy on Facebook*, which provides step-by-step instructions on how to use the privacy settings on Facebook.

The IPC’s excellent working relationship with Facebook has allowed us to influence the site’s privacy practices as they evolve over time. In December 2007, for example, the IPC wrote to Facebook to express strong concerns about its new Beacon ad service program. Beacon, which ultimately stirred great controversy among Facebook users, tracks subscribers’ activities on external partner websites and publishes this information on news feeds that can be viewed by the subscriber's social network. The tracking continues even when users have logged off of Facebook and declined to have their activities published on news feeds.

As a result of the IPC’s intervention and the criticism of other privacy advocates and users, Facebook eventually decided to offer its users the choice to opt out of Beacon altogether.

The IPC strongly believes that building collaborative relationships with website operators such as Facebook puts us in a better position to influence how privacy safeguards are shaped and delivered and to inform users about their privacy choices.
II Education and Outreach

Teacher’s Guides
The IPC has been working to educate students about open government and privacy within the school system for several years, evolving a variety of resources that support deeper awareness and understanding. Our elementary and secondary school program, *What Students Need to Know about Freedom of Information and Protection of Privacy*, is designed for students in grades 5, 10, 11 and 12. It provides guidance to teachers on delivering classes and activities that focus on the concepts of freedom of information and personal privacy.

In 2008, we updated the grade 10 teacher’s guide to include a module about online social networking. The module focuses on the potential privacy implications of posting personal information to a social networking site, and helps students understand the options they have to limit who has access to information about them.

iCommish
In October 2007, Dr. Ann Cavoukian participated in *The Revealed “I”: A Conference on Privacy and Identity*, hosted by prominent privacy researchers at the University of Ottawa. The conference brought together research talent and experts from academic, public, private, and not-for-profit sectors to discuss the impact of information and authentication technologies on identity.

For the purposes of the conference, the Commissioner, along with the privacy commissioners of Alberta and British Columbia, was asked to create a Facebook profile and live a “second life” on Facebook over the summer of 2007. The commissioners were then asked to discuss the results of their group experiment at the conference on a panel called “iCommish.” Dr. Cavoukian offered her tips for keeping Facebook profiles as private as possible, and expressed concerns, shared by the other commissioners, that personal information posted on Facebook could be easily accessed and used for purposes other than social networking (i.e., harassment, stalking, law enforcement, employer checks, etc.). The panel generated interesting and lively discussion that highlighted the risks associated with social networking sites, but also identified the value of Facebook as a means of expressing identities online.

School Outreach
As part of its outreach activities, the IPC visits elementary and secondary schools to speak directly to students about the privacy risks inherent in online activities. The focus is on helping students to understand their responsibility to protect their own online privacy, and on helping them understand the options available to help them do this. In our experience, these face-to-face meetings are highly effective.
We’ve visited a number of schools, including Havergal College, The York School and Earl Grey Senior Public School in Toronto. Sometimes the focus is quite specific. For example, in December 2006, the Commissioner was invited to speak to students and parents at Toronto’s Bishop Strachan School, which was experiencing troubling incidents of cyberbullying in social networking sites and e-mail. Following the presentation to the students, the Commissioner met separately with parents, most of whom were unfamiliar with cyberbullying and other risks that online technologies present.

**Media Interviews**
The media has an important role to play in raising public awareness of issues associated with social networking sites. The IPC regularly makes itself available for media interviews, providing tips about online privacy protection and highlighting its extensive information resources.

**Youth Privacy Online: Take Control, Make It Your Choice!**
Conferences provide good opportunities to build awareness about online privacy issues and explore possible solutions.

In September 2008, the IPC hosted a conference in Toronto entitled *Youth Privacy Online: Take Control, Make It Your Choice!* The conference focused on the privacy risks that young people are exposed to when they use online communication tools, and looked at various methods of safeguarding personal information online.

Speakers included recognized leaders in the fields of research, education, parent advocacy, and technology. Opening remarks were made by Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario, the Honourable Kathleen Wynne, Ontario Minister of Education, and Parry Aftab, well-known Internet safety advocate and lawyer. Presentations were also made by several Canadian researchers, representatives from the education sector, and technology representatives from Facebook, Microsoft, and Research in Motion. A rousing keynote address was delivered by Barbara Coloroso, internationally renowned parent advocate and author. She gave the audience entertaining and insightful advice about teaching children to think critically and ethically when faced with challenging situations.

Conference participants came away with a clearer understanding of the role that online social networking plays in the lives of young people, helping them learn, collaborate, and empower themselves. They also learned that youth may have a unique perspective on online privacy that permits open sharing of personal information within defined networks. While participants shared a sense that technology solutions will continue to evolve, providing better safeguards for personal information online, it was clear to all that these solutions will never take the place of sound judgement and effective parental guidance.
The conference proved to be a valuable learning opportunity for both speakers and participants, and sparked considerable media interest. It was an important step in focusing on the unique issues faced by young people in the online world.

**Teenangels**

Peer-to-peer models for spreading the message about privacy to young people hold tremendous potential. Youth often see their peers as more credible sources of information, and may be more motivated to learn from them than from other authority figures.

That’s why, in 2008, the IPC helped form the first Toronto Chapter of Teenangels. Founded by Parry Aftab, well-known cyber lawyer and Executive Director of WiredSafety.org, Teenangels is a charitable program that trains 13- to 18-year-old volunteers to educate other teens, younger kids, parents, and teachers about online safety, privacy and security.

In the course of their training, members of Teenangels participated in the IPC’s conference *Youth Privacy Online: Take Control, Make It Your Choice!* and helped deliver workshops on online privacy and cyberbullying to students.

**Bacchus Canada**

In trying to reach out to young people, the IPC recognizes the value in working together with organizations that have a similar interests in youth and youth issues. In September 2008, Bacchus Canada asked Commissioner Cavoukian to tape a public message for its student awareness campaign on online social networking.

Bacchus Canada, a division of The Student Life Education Company, is a non-profit organization that seeks to promote healthy decisions about alcohol and other health issues among post-secondary students.

Dr. Cavoukian’s video message, which has been posted on Bacchus Canada’s Facebook page, urges viewers to be proactive about protecting their privacy online, and to educate themselves about the privacy controls available on social networking websites.
III National and International Initiatives

Resolutions on Children's Online Privacy
On June 4, 2008, the IPC joined its counterparts across Canada in endorsing a Resolution on Children’s Online Privacy. The Resolution, among other things, calls upon Canada’s privacy commissioners to work collaboratively on developing and promoting education-based activities, pressing industry to adopt strong privacy standards and urging operators of websites to implement better privacy practices.

On October 17, 2008, at the 30th International Conference of Data Protection and Privacy Commissioners in Strasbourg, France, the IPC and other data protection authorities from around the world endorsed a similar Resolution on Children’s Online Privacy. Like the Canadian version, the Resolution strongly urges data protection authorities to support collaborative, education-based approaches and to encourage operators of websites to adopt privacy-protective policies and measures.

The IPC is committed to the principles set out in the Resolutions, and is pleased that, through its extensive outreach activities, the IPC is already on track to meet or exceed the stated goals. The IPC looks forward to working collaboratively with other data protection authorities to advance knowledge and education in the area of youth online privacy.

Report and Guidance on Privacy in Social Network Services
The privacy and security issues associated with online communities are a matter of global concern. As a member of the International Working Group on Data Protection in Telecommunications, the IPC helped to inform the development of the Report and Guidance on Privacy in Social Network Services ("Rome Memorandum"), which was released on March 4, 2008. The Working Group was initiated by Data Protection Commissioners from different countries in order to improve privacy and data protection in telecommunications and media.

The Rome Memorandum includes a comprehensive list of the known privacy risks associated with the use of social networking sites and guidance on privacy-protective measures for regulators, providers and users of social networking sites. It is an important resource for the public and stakeholders on best practices for safeguarding personal information on social networking sites.
IV Conclusion

The IPC has been extremely active in building awareness of online privacy issues among young people, especially as they related to online social networks. Using a variety of channels and media, our focus has been on helping youth understand risks and empowering them to make conscious choices about when, how, and with whom they share personal information.

Youth, like other demographic groups, can benefit tremendously from the Internet and all it has to offer. But they must do so with their eyes wide open, using their judgement to stay in control of their personal information and, ultimately, of their reputations.

The IPC looks forward to further opportunities to help make young people more privacy-savvy when they engage in online activities, and to encourage key stakeholders to make more privacy-enhancing options available online.
How to Protect Your Privacy on Facebook: A Step-by-Step Guide

(Originally published May 3, 2007; most recently updated March 17, 2009)

March 2009
How to Protect Your Privacy on Facebook:
A Step-by-Step Guide

(Originally published May 3, 2007; most recently updated March 17, 2009)

When you sign up as a user of Facebook, the default settings allow all other Facebook users to find you in searches. However, only those you have confirmed as friends or who share a network with you have access to your full profile. By default, your name and thumbnail profile picture can also be found on public search engines. Facebook has selected these settings based on what it believes most users want, but you can always change them to restrict access to your information, as you see fit. Therefore, you can change the default settings to restrict access to your profile. Under the current setting, only your friends, their friends, and the people on your networks can see your profile. If you download Facebook Platform third-party applications into your profile, some of your information may be shared (see section on “Applications” below). It is important to explore these default settings, to adjust the privacy settings to those with which you are comfortable.

It’s easy to change the default settings. Once you sign in, click on “Settings” at the top of the screen toward the right, (just to the left of the Search bar), and then choose “Privacy Settings” from the drop-down menu. The Privacy menu has four categories in which you can determine the degree of privacy you would like. You can click on each heading to access the page on which you can make your changes. Privacy settings can be customized to exclude or include specific friends or lists of friends. Remember to click on “Save Changes” before exiting the page. (Note: Review your privacy settings if you change regional networks. The settings will change back to the default: all members of that network will be able to see your full profile. It is important to be aware of this, and adjust your privacy settings if this is not what you want. It is a wise practice to check your privacy settings whenever you add anything or make changes to your profile.)

Profile: This page contains two tabs, each with numerous individual controls for who can see aspects of your profile. On the Basic tab are controls for your entire profile, and individual features of your profile: Basic Information (which includes Gender, Birthday, Hometown, Political and Religious Views, and Relationship Status), Personal Information (which includes your Interests, Activities, Favorites and your About Me section), photos and videos tagged of you, status updates, friends, wall, education and work information. On the Contact Information tab, you can tailor permissions for IM Screen Name, Mobile Phone, Phone, Current Address, Website and Email Address (if in fact you provided these details for your profile).
Privacy by Design

- To limit viewing of Profile information to only your Facebook friends, select "Only Friends" in each drop-down menu. If you wish to limit viewing to certain segregated lists of friends that you can set up on your main Friends page, or just to individual friends, or to exclude certain individuals and networks, choose "Customize" in the drop-down menus and adjust the settings accordingly.

**Search:** You can control which Facebook users can find you in searches and what appears in your search listing within the site; you can prevent yourself from being suggested as a prospective friend to other Facebook users in the "People You May Know" feature; you can also control whether you are searchable by anyone on public search engines. Within Facebook, you can restrict which networks have access to your profile in searches and what actions people can take with your search results, such as contacting you or adding you as a friend.

- To be searchable within Facebook only by your Facebook friends, select "Only Friends" in the Search Visibility drop-down menu and leave the first set of checkboxes below the drop-down menu (the ones starting with "In addition...") blank.

- "Only Friends" also works to prevent your being presented as a prospective friend to other Facebook users. If you are available in Search to someone (for example, "Friends of Friends," "My Networks and Friends of Friends," or "Everyone") you may appear in their "People You May Know" section. You will also not be presented as a potential friend to anyone you have "x-ed out" of "People You May Know."

- To avoid being searchable on public search engines (Yahoo, Google, etc.), if you have selected "Everyone" in the Search Visibility drop-down menu, simply uncheck the box next to "Create a public search listing for me." Unchecking this box also makes basic information about you (your name, networks, profile picture and friend list) unavailable to Facebook Platform applications.

**News Feed and Wall:** This page has two tabs. On the "Actions within Facebook" tab, you can control what activities result in stories showing up automatically on your Wall and your friends’ News Feeds.

- "Uncheck" any actions that you do not want your friends to know about automatically, such as when you make a comment on a posted item or add a friend.

On the "Social Ads" tab, you can opt out of your information (and photos) being used for ads targeted at your friends by choosing "No One" in the drop-down menu.

**Applications:** You can place some controls on the information available to applications on your account, including those built using the Facebook Platform. Third-party applications, however, may have their own privacy policies and user controls that prevail over your Facebook settings. As stated in Facebook’s Terms of Use,
these applications are used at your own risk. You can learn more about applications by reading the "Overview" tab in this section.

- Under the "Settings" tab, you can set controls for any applications installed by your friends, and a general opt-out from any information being shared through the Facebook Platform. For maximum privacy protection, you can check off "Do not share any information about me through the Facebook API." Please note that this option will automatically switch off if you download any third-party applications or use your Facebook log-on and password to sign up on an external website with Facebook Connect. In other words, downloading applications means that information about you may be shared in ways you cannot control.

- This page lists any applications you have blocked, and is where you can unblock them. You can also keep track of friends whose application invitations you ignore on this page.

- The "Beacon Websites" checkbox lets you opt out of having certain external websites post stories to your Wall and your friends’ News Feeds about your activities on those sites. You can essentially opt-out by going to the “Settings” tab on the Applications privacy page and under “Beacon Websites” check the box "Don’t allow Beacon website to post stories to my profile". Checking this box will ensure that no Beacon site ever publishes a story to your profile.

- To view a summary and to change your own Application permissions, click on the “Applications” button in the bottom-left corner of any of your Facebook pages, then click on “Edit” in the pop-up window. In the chart displayed, each application has its own “Edit Settings” option available. This brings up a selection of choices about permissions to publish stories on your Wall about your activities on the application or Facebook Connect external website. For maximum privacy, select “Never publish any stories from…”

In addition, the Privacy Overview page offers the option of blocking specific people from viewing your profile. Under “Settings” from any Facebook page choose “Privacy” from the drop-down menu to access the “Block People” prompt.

Elsewhere on Facebook, you can control who can see notes you have written and photos you have posted, and manage the visibility of your online status.

- Within “Notes”, click on either the “My Notes” or “Notes About Me” tab and click on the “Edit Notes Privacy” link under the Notes Settings heading on the right side of the page. The drop-down menu has the same options as those for Profile components explained above. You can also establish settings for who can comment on and subscribe to your notes.

- Within “Photos”, click on “Album Privacy” to adjust drop-down menus for each album, in the same manner as the Profile components explained above.
To adjust your online status setting, click inside the small Chat box that contains a silhouetted head and shoulders in the bottom right corner of your Profile page. A small pop-up menu will appear including a row with a statement of your online status. You can click to appear offline (represented by a red dot) even if you are online. If your status is shown as online (green dot), your friends who investigate this feature can discover that you are online. This feature is intended to facilitate chat.

To report an impostor profile on Facebook:

- From any Facebook page, go to the Privacy Help Page in the Help Center. One way to get to the Privacy Help Page is to click on the “Help” or “Privacy” link in the bottom right-hand corner. In the Privacy Questions and Answers, Abuse section, click on “I need to report an impostor profile”. To complete the email form, the following information is requested: your contact email address; URL of the profile you would like to report; the full name of the person you would like to report; Networks the profile belongs to; the email address listed for the profile; and a description of the issue.

- You can also get to a general Contact Us form by clicking on “Help”, then “Security”, then “How Do I Report Abuse”, and finally “My Question is Not Listed”. Complete the email form, specifying that you are reporting an impostor profile.

Additional IPC Resources

When Online Gets Out of Line – Privacy: Make an Informed Online Choice
This brochure encourages university, college and high school students to carefully consider their privacy options.

Be a Player: Take Control of Your Privacy on Facebook
In this video, Commissioner Cavoukian discusses privacy and security issues with regards to online social networking.
Reference Check: Is Your Boss Watching?
Privacy and Your Facebook Profile

February 2009
Reference Check: Is Your Boss Watching?
Privacy and Your Facebook Profile

Facebook and other online social networks are the web destinations of choice for more and more people to connect, communicate, and share personal information with others. While they may have started out as networking and recreational tools for young people, the large online social networks now attract people of all ages.

The practice of employers looking for background information about job candidates on social networking websites such as Facebook is also growing. These sites are now being used as a business tool by hiring managers who see their potential, along with search engines, for background checks on potential employees. Users of Facebook and other such sites should post information with their eyes wide open – considering the risks to their employment prospects, current and future. This paper will suggest ways of mitigating and minimizing such risks.

It’s crucial to remember that anything posted online may stay there forever, in some form or another. Whether through the Internet Archive’s Wayback Machine site, or the caches of Google and Yahoo, old versions of websites are indeed searchable by those who know how. What is actually found may include your own material, as well as information about you, posted by others at other sites. This uncertainty regarding one’s privacy and confidentiality of sensitive information is a major downside to social networking sites, despite their many positive aspects. Anything associated with you – or the people you are connected to – can and most likely will be viewed and evaluated by other people, some of whom may have considerable influence over your life, now or in the future.

When you realize that information about you on the Internet may be used in a work-related context, you may see things in a different light. Depending on what

---

1 According to comScore, considered the global leader in measuring the digital world, Facebook became the largest of the top 10 gaining properties in terms of monthly unique visitors, in May 2007, with at least five times more visits per visitor than any of the others in the top 10 fastest growing sites.

2 A recent Canadian poll of Internet users found that one-third of online Canadians aged 50 and over have visited social networking sites. For those in their 40s, it’s 45%.

3 In survey data from ExecuNet, 77% of executive recruiters used web search engines to research candidates and 35% said they had ruled out candidates on that basis.


4 http://www.archive.org/web/web.php
information is posted, it could seriously harm, or help, your prospects. Users of mass-market sites such as MySpace, Facebook and Friendster may feel that anything goes and “free speech” should prevail since they are just chatting amongst “friends.” And they may feel that as part of a closed network – a school or a geographic region, they have some built-in privacy protection. Both views are mistaken. Consider the following:

- January, 2007 – Farm Boy, an Eastern Ontario grocery chain, fired several employees from its Ottawa store after learning of the content of postings on a “I got Farm Boy’d” group on Facebook. A former employee was quoted in the Ottawa Citizen as saying that he was accused of stealing from the store, based on his posts on the group page.

And it’s not only current employers who may be looking at your network content. It’s your potential future boss, or someone who might never become your boss if he or she finds certain material offensive or even troubling, and decides not to interview you as a result. Recruiters can – and do – use search engines and social networks to gather background information on job candidates, and many are beginning to eliminate candidates based on what they find. (Facebook has made this even easier by allowing limited member profile information to be searchable on public search engines, but members can prevent this by using their privacy controls.) They might see or read things they would not be allowed to ask you about in an interview, due to human rights laws. So if you’re going to post sensitive information on your site, you should be prepared to answer questions about any issues relating to your online profile.

Here are a few examples of the types of things that might cause concern and raise questions for employers researching you:

- Your recreational activities captured in photos on your profile and your friends’ profiles:
  - If you appear drunk or out of control, “partying” or otherwise engaged in behaviour that may be considered offensive, your reputation could suffer.

- Your comments about employment situations:
  - “I hate my boss!”
  - “I was late for work again today. I just can’t get out of bed!”
  - “I shouldn’t have to work so hard!”

5 Facebook networks offer a minimal level of privacy in that profiles of users in other networks cannot be viewed unless they have linked with you as a friend. But it is a simple matter to temporarily join the regional network of a research target in order to try and view that target’s profile information, if it is not protected by applying additional privacy settings.

6 See the IPC’s tipsheet “How to Protect Your Privacy on Facebook,” http://www.ipc.on.ca/images/Resources/up-1facebk_handout_priv.pdf
Your religious, political, or sexual activities or views (stated or implied through membership in groups):
- If they vary significantly from the mainstream, beware of their potential impact.

If decisions about you are made based on information obtained from social networking websites, you may never know why you didn’t get the job, the interview, or the promotion. At least for now, those decisions are likely being made by individuals for whom the “tell all” nature of Web 2.0 tools, like social networking sites, still seem foreign, embarrassing, risky, or even seriously misguided in the business world.7 What you might see as fun and meaningless in a “Wall” post or photo could be interpreted as evidence of recklessness and lack of judgement by someone who doesn’t understand the context. Your activities, comments, and views, even though you may have just been joking around with your friends, all become part of an online résumé that, inadvertently or not, becomes available to everyone.

What can you do to protect yourself – to avoid embarrassment and, worse, loss of employment opportunities?

1. “Think hard before you click” to post text or photos to groups or discussion boards or write on anyone else’s pages, in ways or on topics that you would not want to discuss with your current employer, or in a job interview. Inappropriate, demeaning or defamatory comments related to your work are particularly risky.

2. **Review** what is out there about you, on social networking sites, on customized business and HR sites such as ZoomInfo and LinkedIn, and through search engines such as Google. Some of it might be completely fictional. Others may refer to someone with the same name as you, but you need to know about it.

3. **Remove**, if possible, anything you would not want to discuss with your current employer, or in a job interview; ask friends to take down items such as questionable photos of you. There are now private services available, such as Reputation Defender (www.Reputationdefender.com) that offer to do this for you, for a fee.

But be aware that the effects of some information may continue:
- Information removed could still live on in cached or archived copies of the website, which can be located by Internet users who are determined to find them. Be prepared to explain any of the deleted material;

---

– It will be almost impossible to have material removed that has found its way into news media or government records;

– Damaging information may have already been viewed by potential employers;

4. **Implement privacy controls** over your personal information on online social networks. These can be tricky to use, so once you’ve set them up, make sure you test them out – have someone try to look at your profile or search it yourself on a public search engine.\(^8\)

– Remember that if viewers of your profile can also view your friends’ pages, they may see images and read remarks you’d rather they didn’t. You should also ensure that your profile is not visible to viewers of your friends’ pages and, if possible, apply appropriate privacy controls – Facebook has several – to ensure that photos of you on other people’s pages are not “tagged” with your name.\(^9\)

– Be extra careful with applications created by third parties within social networks. These applications (such as iLike) may collect your personal information, and unless you locate and agree to their privacy policy (and they adhere to it), you may have no idea what might be done with that information.

5. **Build up a positive image** for yourself on your profile through comments on your own and others’ sites, photos, and groups – that’s what you want prospective employers to see.

Finally, we have to say it again, but it bears repeating – the Internet, the web is a fundamentally public place. If you can’t get rid of something, assume it’s going to be seen and be ready to explain it.

---

\(^8\) Do not rely absolutely on these controls; they may change without your being informed.

\(^9\) See the IPC’s tipsheet “How to Protect Your Privacy on Facebook,” [http://www.ipc.on.ca/images/Resources/up-1facebk_handout_priv.pdf](http://www.ipc.on.ca/images/Resources/up-1facebk_handout_priv.pdf)
CONTACT INFORMATION:

General inquiries should be directed to:
Tel: (416) 326-3333
1-800-387-0073
Fax: (416) 325-9196
TTY (Teletypewriter): (416) 325-7539
E-mail: info@ipc.on.ca
Website: www.ipc.on.ca

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

Ann Cavoukian, Ph.D.
INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO
CANADA

PRIVACY BY DESIGN
...TAKE THE CHALLENGE

Ann Cavoukian, Ph.D.
INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO
CANADA

CONTACT INFORMATION:

General inquiries should be directed to:
Tel: (416) 326-3333
1-800-387-0073
Fax: (416) 325-9196
TTY (Teletypewriter): (416) 325-7539
E-mail: info@ipc.on.ca
Website: www.ipc.on.ca

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

Ann Cavoukian, Ph.D.
INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO
CANADA