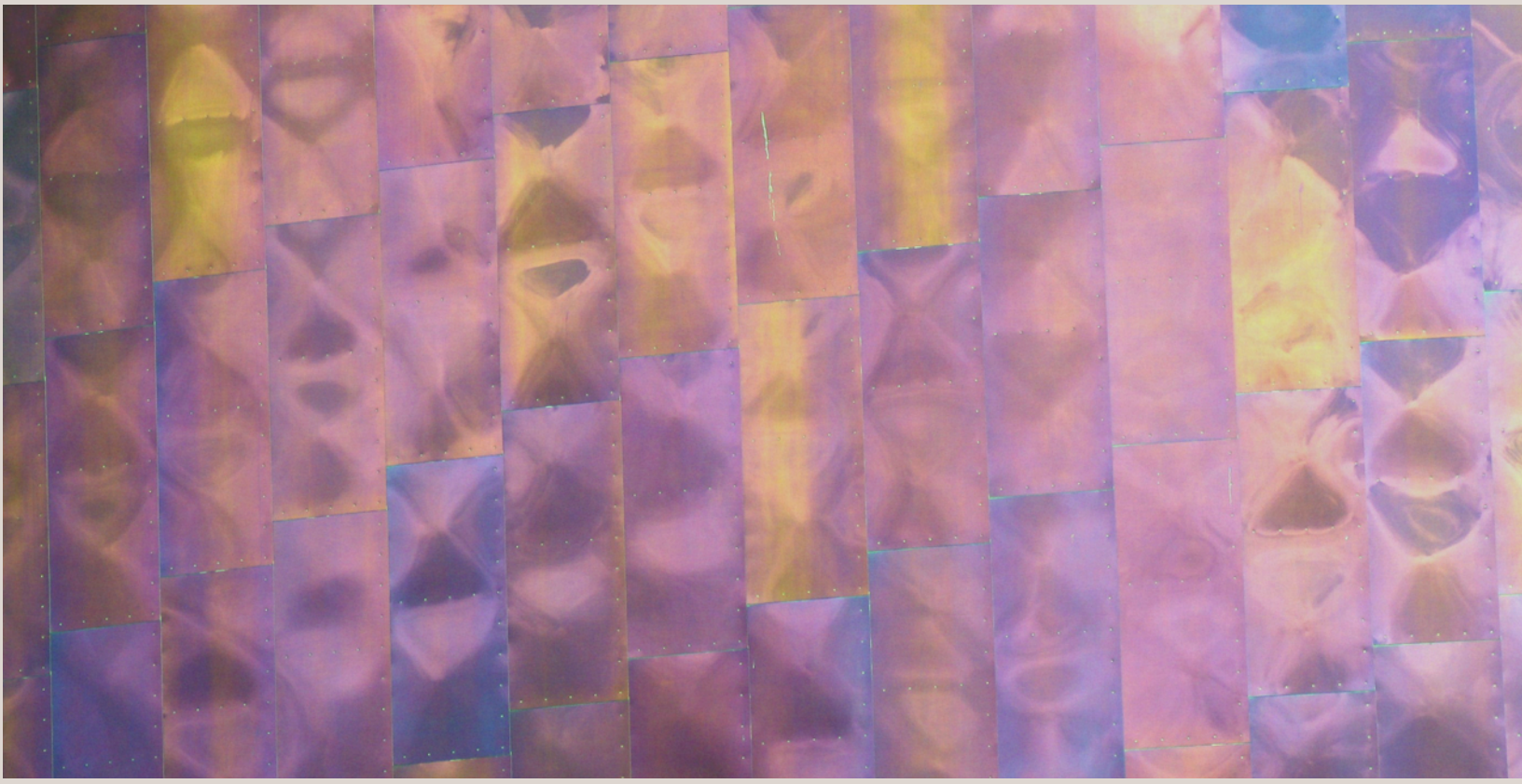
Privacy
AND
Radical Pragmatism:



Change the Paradigm

A White Paper

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

August 8, 2008

Table of Contents

Foreword **1**

Radical Pragmatism **3**

Creating Positive-Sum Solutions 4

Transformative Technologies 5

Context **6**

Surveillance Technologies 7

Zero-Sum Security? 8

Foundations of Radical Pragmatism **9**

The 'Privacy Payoff' 10

"Privacy by Design" — Build it in Early on 11

Privacy-Enhancing Technologies (PETs) 12

Best Practices in Information Management and Governance 13

Applied Radical Pragmatism **14**

Examples of Transformative Technologies **16**

1. Biometric Encryption 17
2. Radio Frequency Identification (RFID) 18
3. Video Surveillance Image Encryption 20
4. Privacy Enhanced Network Tracing and Monitoring 21
5. Whole Body Imaging 21
6. Private Digital Identities 22
7. Privacy-enhanced Age Verification 24

Endnote: Commissioner's Message **24**

IPC References **25**

Biometric Encryption 25

Radio Frequency Identification (RFID) 25

Video Surveillance 25

Online Privacy 26

Privacy and Security 26

Identity Theft 27

Miscellaneous 27

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.

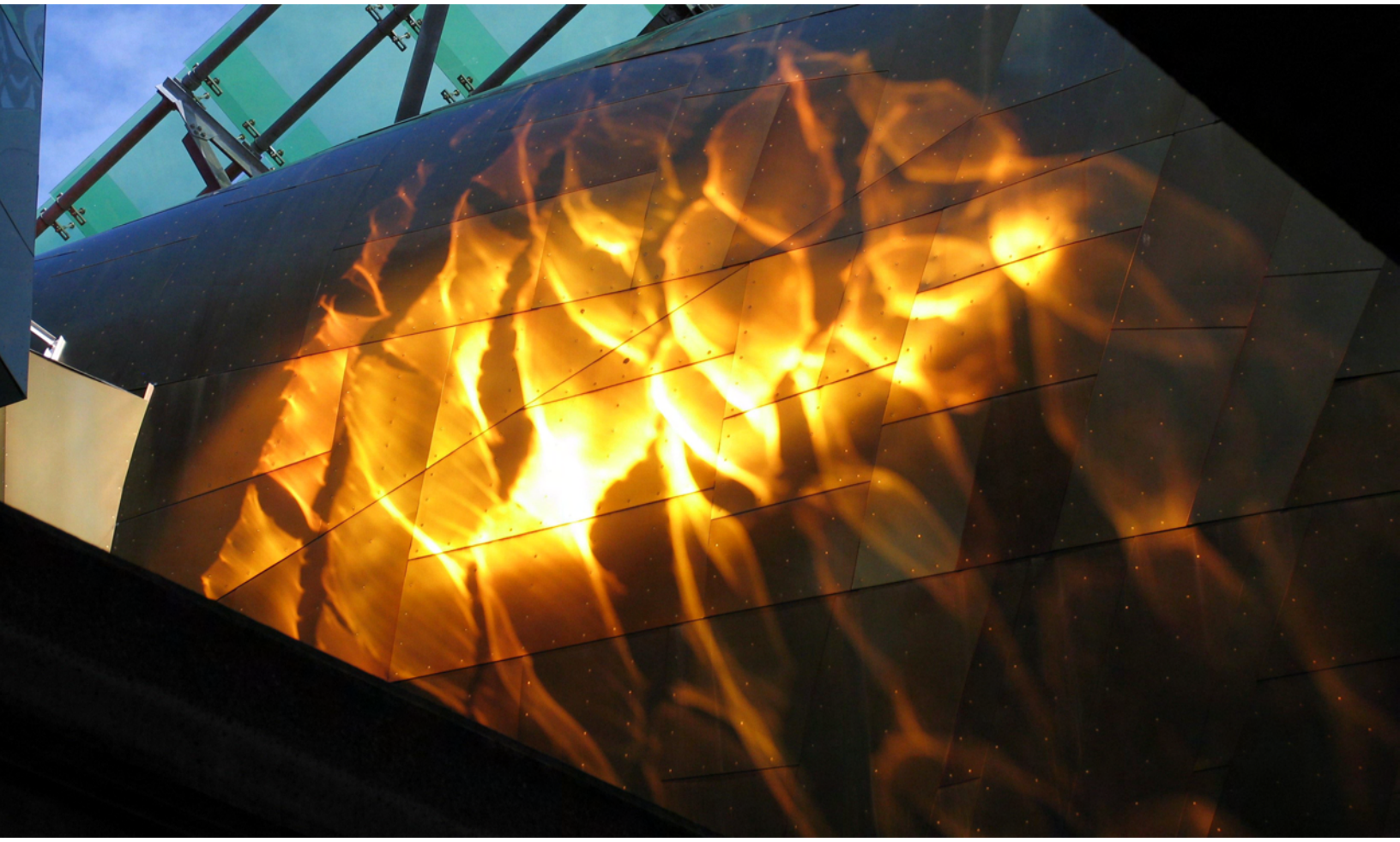
Some say that privacy is fast becoming an outdated concept, a function more of default practical obscurity than of ongoing societal debate and consensus. I'm not one of those people. It's hard to believe that, twenty years ago, the debate raged on for years about the privacy pros and cons of caller ID 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

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.



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, but also 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).

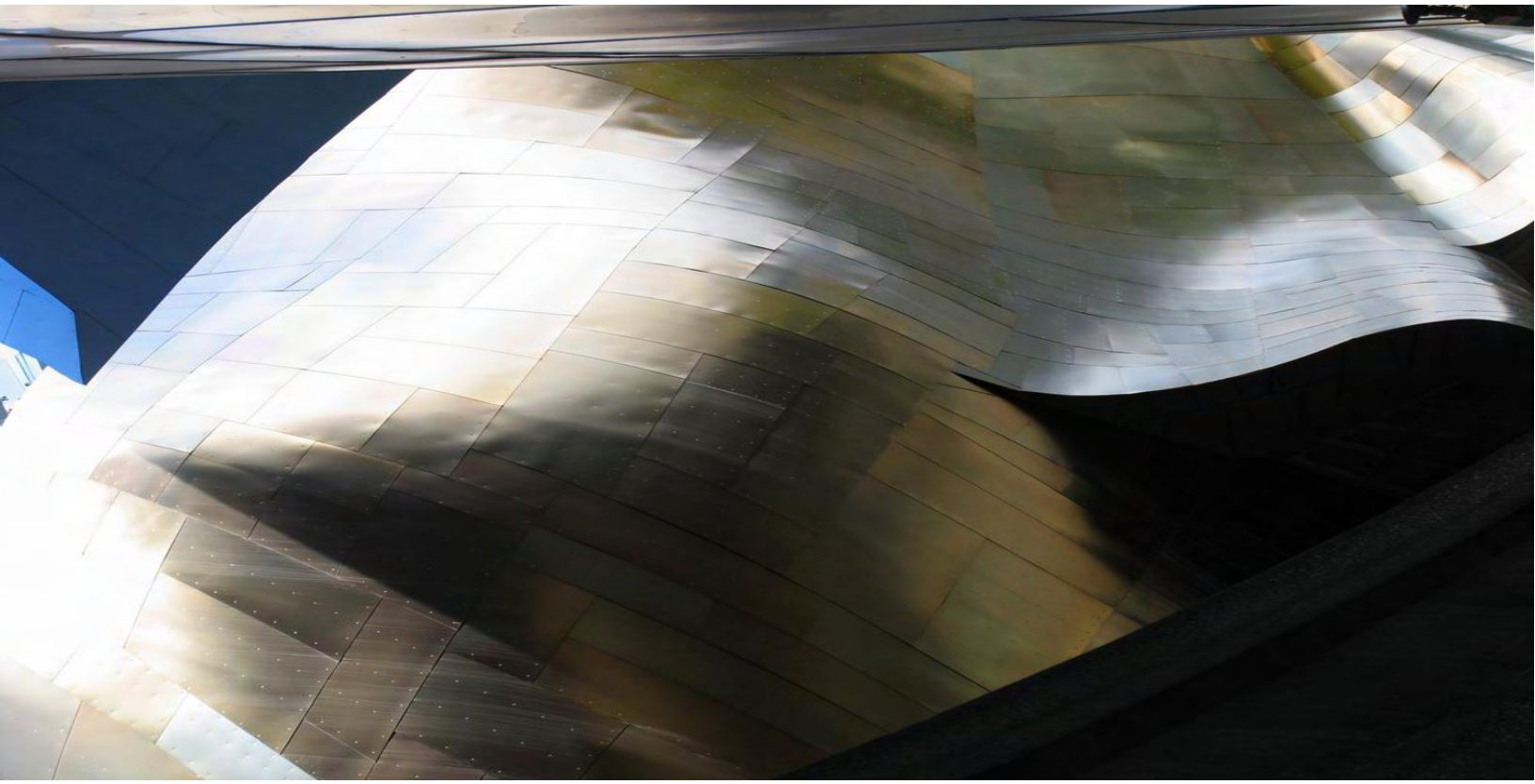
To achieve a positive-sum model, privacy must be proactively built into the system, so that privacy protections are engineered directly into the technology, right from the outset. I call this "privacy by design". The effect is to minimize the unnecessary collection and use of personal data by the system, 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, that 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_



Context

"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 towards 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 offline, 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, I 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 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 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 action[2]. 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 pragmatisms explicitly recognize 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:

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."

"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.

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 behavior are borne by others (negative externalities).

---

3 *The Privacy Payoff: How Successful Businesses Build Customer Trust*, Ann Cavoukian, Ph.D. and Tyler J. Hamilton www.privacypayoff.com

4 For a greater discussion, see IPC Publication, *Privacy and Boards of Directors: What You Don't Know Can Hurt You*, at www.ipc.on.ca/docs/director.pdf

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.

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."[6]

"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 towards 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.

5 *The Privacy Payoff: How Successful Businesses Build Customer Trust,* Ann Cavoukian, Ph.D. and Tyler J. Hamilton www.privacypayoff.com

6 Bruce Kasanoff, *Making it personal: how to profit from personalization without invading privacy* (Perseus, October 2001), p.65

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.

Privacy-Enhancing Technologies (PETs)

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."[7] 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.

7 Kenny S and Borking J, *The Value of Privacy Engineering*, Refereed Article, The Journal of Information, Law and Technology (JILT) 2002 (1) http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_1/kenny/

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.

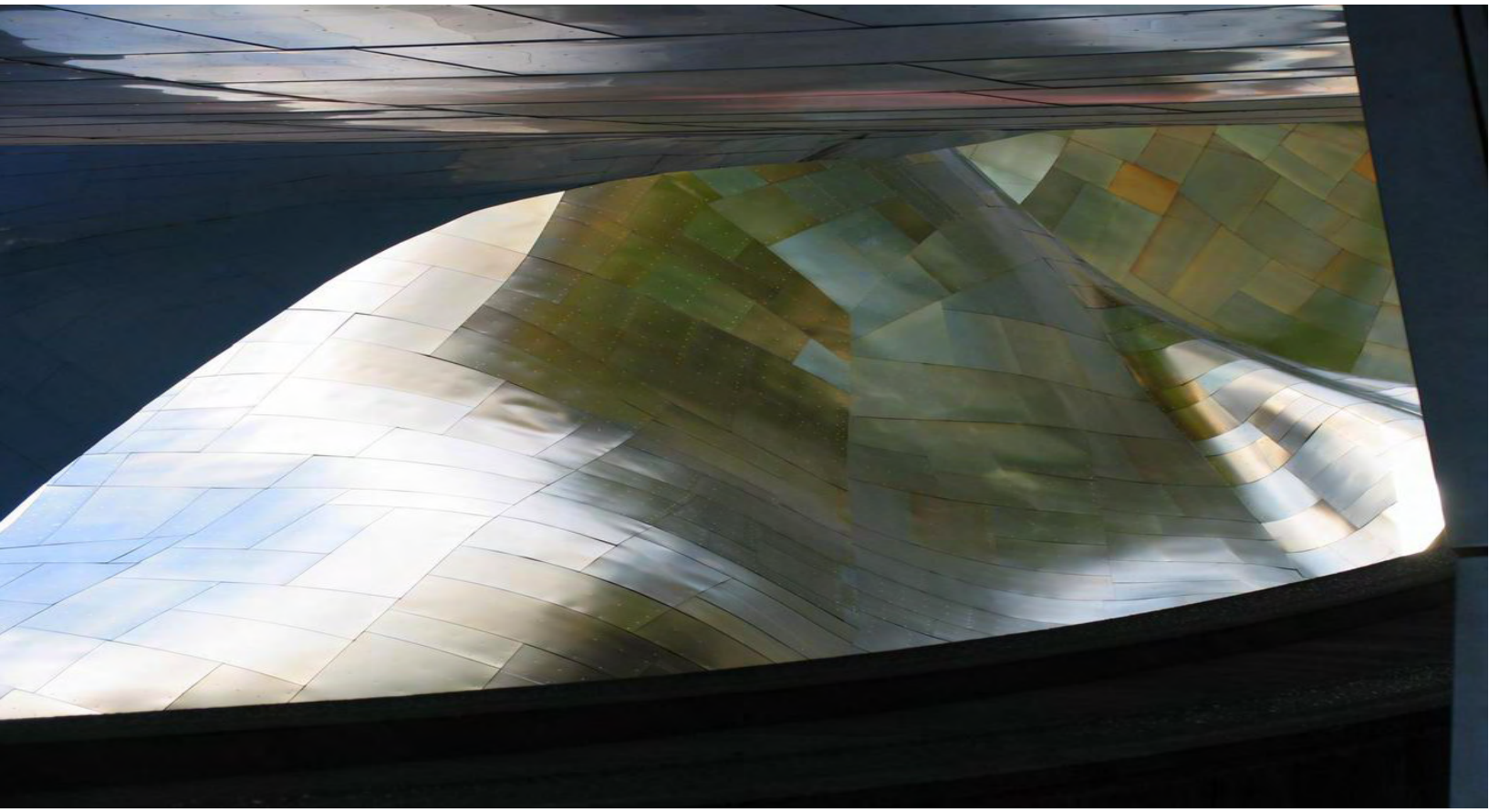
Considerable effort has also been vested in raising public awareness and education among all privacy stakeholders, from making available privacy tutorials for use in primary and secondary schools to publishing tip sheets on how to protect your privacy for Facebook users, offering assistance to identity 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

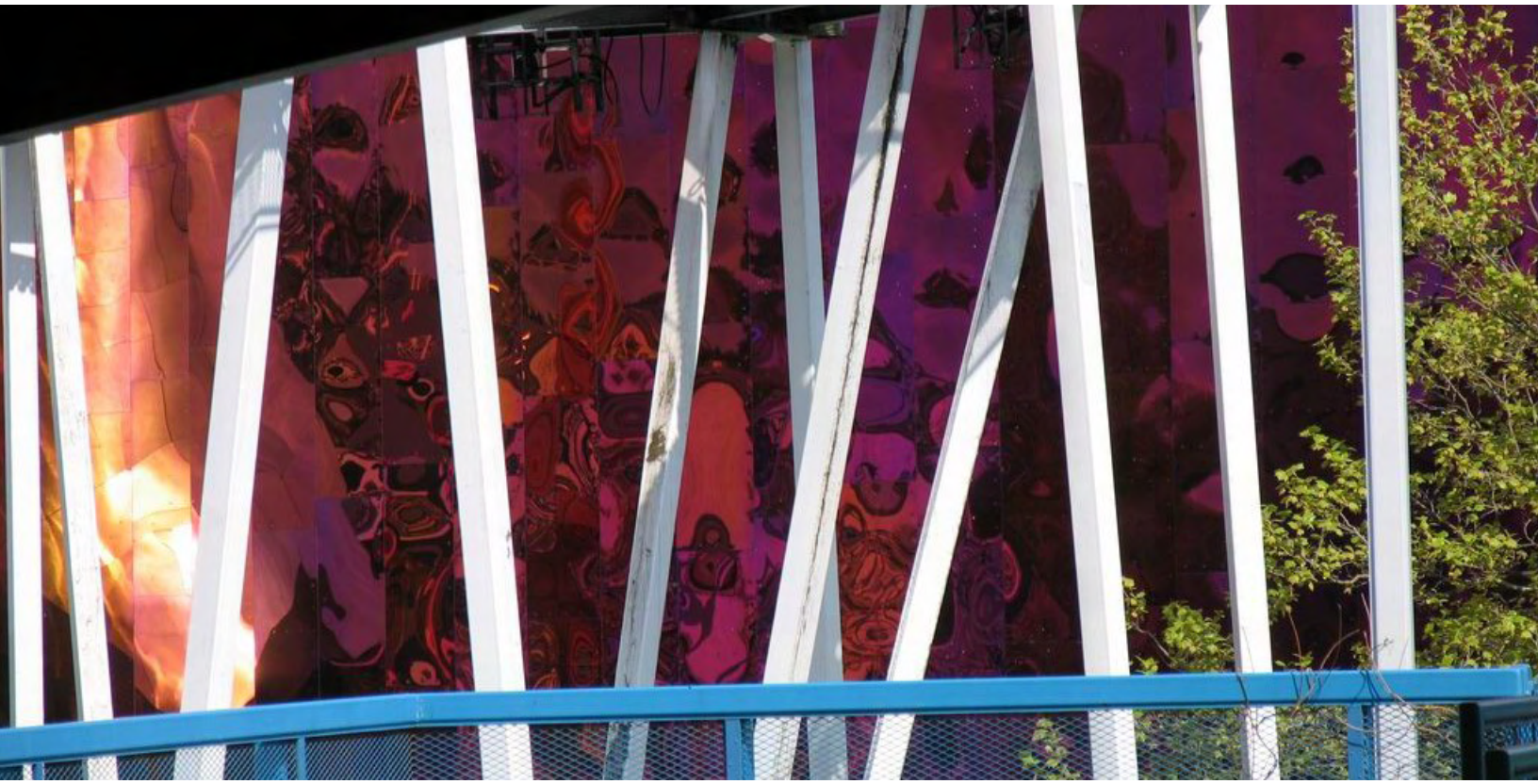
and commerce; to ensure that public agencies are held accountable for their actions; and, more generally, to ensure that personal data is collected, used, retained and shared in a manner that is open, transparent, equitable, in accordance with the interests of individuals and, above all, to serve redeemable 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
7. Privacy-enhanced age verification

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, present 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 cancelable 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 **F**requency **ID**entification tags are the next generation technology beyond barcodes. RFID tags contain microchips and tiny radio antennas that 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.

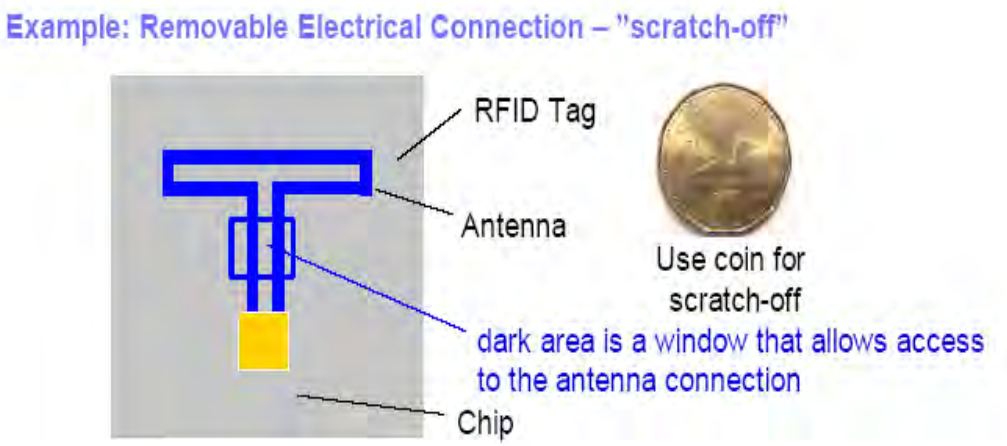
However, the growing practice of tagging consumer products also raises many privacy and security concerns, especially when the tagged items being scanned are linked to identifiable individuals. The prospect of hidden, unauthorized readers scanning the personal items we carry about with us —such as our prescription vials, clothing brands, styles and sizes, or books we are reading— without our

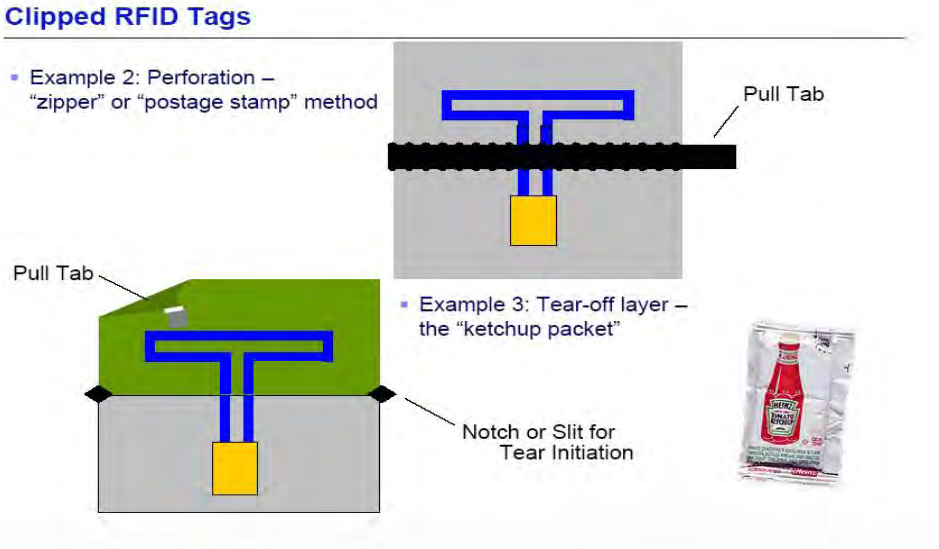
8 Available at: www.ipc.on.ca/index.asp?navid=46&fid1=608&fid2=4

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.

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.

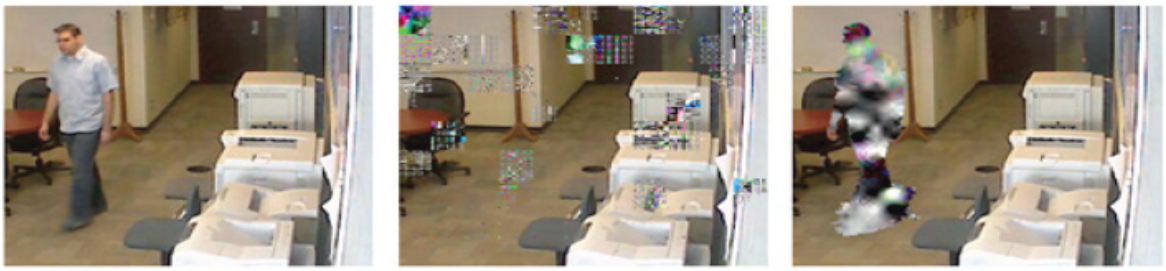
However, when deployed in a transparent and accountable manner, video surveillance cameras can help achieve valid objectives, such as crime detection and preserving evidence in the event of an incident. Nonetheless, valid concerns remain about how the recorded images will be used, what assurances people 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.

9 See P*rivacy Protected Surveillance Using Secure Visual Object Coding*, Martin, K.; Plataniotis, K.N., Digital Object Identifier: 10.1109/TCSVT.2008.927110, IEEE Transactions on Circuits & Systems for Video Technology, August 2008, to be published.



(a) (b) (c)

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.

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[10]. 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.[11]

Researchers at the University of Toronto have created a technology called "Bunker" that allows ISPs to securely trace their networks.[12] 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.

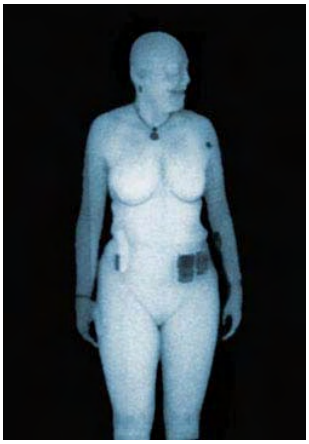
5. Whole Body Imaging

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.'

10 http://www.cbc.ca/money/story/2008/02/12/bell.html
11 http://blog.wired.com/27bstroke6/2008/07/judge-orders-yo.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

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.

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).



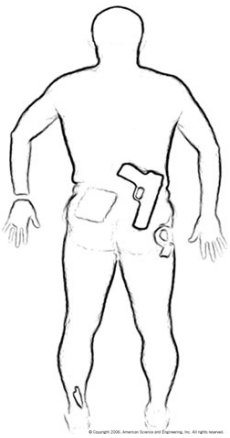


Figure 1: Sample raw backscatter image
Figure 2: Backscatter image, after privacy algorithm applied (note: different sample scan)

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 offline 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 offline 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.[13] 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/

7. Privacy-enhanced Age Verification

It is becoming increasingly common in the offline world for the personal details stored on one's government-issued identity credentials, such as a driver's licence or other identity document, to be automatically scanned, swiped or otherwise recorded as a condition of various encounters: returning a product for refund, cashing a lottery ticket, purchasing cigarettes, or even entering a club. This recording is often required, not only to validate the age or identity of the cardholder, but to satisfy existing legal due diligence requirements by creating a log and audit trail to prove that identity or age was, in fact validated.

Immediate privacy risks and problems associated with over collection, storage and misuse of personal identity data, present themselves. In many jurisdictions, personal information such as one's name, home address, licence number, date of birth, sex and height is encoded on the magnetic strip on the reverse side of a driver's licence card. There is little reason why most, if not all of this data ever needs to be collected or retained.

Fortunately, technology can help. Special trusted card readers have been developed by Ontario firms [such as Legalese] and are being deployed at various point-of-sale locations. When swiped with an identity card, such as a driver's licence, these age verification boxes are able to provide instant age verification without any need to actually record or retain the data in question. They also relieve the need to manually ensure that the card isn't a forgery or hasn't been tampered with (see **www.legalage.ca**). This is another example of innovation in technology that achieves both strong privacy and its intended functionality – win/win.

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.

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

Fingerprint Biometric Systems: Ask the Right Questions Before You Deploy. July 2008. http://www.ipc.on.ca/index.asp?navid=46&fid1=769

Biometric Encryption: A Positive Sum Technology that Achieves Strong Authentication, Security AND Privacy. March 2007. 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)

RFID and Privacy: Guidance for Health-Care Providers. January 2008. http://www.ipc.on.ca/index.asp?navid=46&fid1=724

Commissioner Cavoukian issues RFID Guidelines aimed at protecting privacy. News Release. June 2006. http://www.ipc.on.ca/index.asp?navid=55&fid1=427

Privacy Guidelines for RFID Information Systems (RFID Privacy Guidelines). June 2006. http://www.ipc.on.ca/index.asp?navid=46&fid1=432

Practical Tips for Implementing RFID Guidelines. June 2006. http://www.ipc.on.ca/index.asp?navid=46&fid1=430

Guidelines for Using RFID Tags in Ontario Public Libraries. June 2004. http://www.ipc.on.ca/index.asp?navid=46&fid1=410

Tag, You're It: Privacy Implications of Radio Frequency Identification (RFID) Technology. February 2004. http://www.ipc.on.ca/index.asp?navid=46&fid1=319

Video Surveillance

Privacy Protected Surveillance Using Secure Visual Object Coding, Martin, K.; Plataniotis, K.N., Digital Object Identifier: 10.1109/TCSVT.2008.927110, IEEE Transactions on Circuits & Systems for Video Technology, August 2008, to be published.

Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report - Privacy Investigation Report MC07-68. March 2008. http://www.ipc.on.ca/index.asp?navid=53&fid1=7874

Guidelines for the Use of Video Surveillance Cameras in Public Places. Updated September 2007 http://www.ipc.on.ca/index.asp?navid=46&fid1=647

Fact Sheet #13: Wireless Communication Technologies: Video Surveillance Systems. June 2007. http://www.ipc.on.ca/index.asp?navid=46&fid1=626

Privacy Review: Video Surveillance Program in Peterborough. December 6, 2004. http://www.ipc.on.ca/index.asp?navid=46&fid1=582

Guidelines for Using Video Surveillance Cameras in Schools. December 2003.
http://www.ipc.on.ca/index.asp?navid=46&fid1=412

Online Privacy

Privacy in the Clouds: Privacy and Digital Identity – Implications for the Internet. May 2008.
http://www.ipc.on.ca/index.asp?navid=46&fid1=748

7 Laws of Identity The Case for Privacy-Embedded Laws of Identity in the Digital Age. October 2006.
http://www.ipc.on.ca/index.asp?navid=46&fid1=471

Privacy and the Open Networked Enterprise. June 2005.
http://www.ipc.on.ca/index.asp?navid=46&fid1=576

EPAL Translation of the The Freedom of Information and Protection of Privacy Act [version 1.1]. March 2004. http://www.ipc.on.ca/index.asp?navid=46&fid1=344

Concerns and Recommendations Regarding Government Public Key Infrastructures for Citizens. December 2002. 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

An Internet Privacy Primer: Assume Nothing. August 2001.
http://www.ipc.on.ca/index.asp?navid=46&fid1=286

Best Practices for Online Privacy Protection. June 2001.
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

Geographic Information Systems. April 1997. http://www.ipc.on.ca/index.asp?navid=46&fid1=345

Privacy and Security

Transformative Technologies Deliver Both Security and Privacy: Think Positive-Sum not Zero-Sum. July 2008. http://www.ipc.on.ca/index.asp?navid=46&fid1=758

Creation of a Global Privacy Standard. November 2006.
http://www.ipc.on.ca/index.asp?navid=46&fid1=575

Cross-National Study of Canadian and U.S. Corporate Privacy Practices. May 2004.
http://www.ipc.on.ca/index.asp?navid=46&fid1=341

Statement to the House of Commons Standing Committee on Citizenship and Immigration Regarding Privacy Implications of a National Identity Card And Biometric Technology. November 4, 2003.
http://www.ipc.on.ca/index.asp?navid=46&fid1=113

The Security-Privacy Paradox: Issues, Misconceptions, and Strategies. August 2003.
http://www.ipc.on.ca/index.asp?navid=46&fid1=248

National Security in a Post-9/11 World: The Rise of Surveillance…the Demise of Privacy? May 2003.
http://www.ipc.on.ca/index.asp?navid=46&fid1=236

Security Technologies Enabling Privacy (STEPs): Time for a Paradigm Shift. June 2002.
http://www.ipc.on.ca/index.asp?navid=46&fid1=245

Commissioner issues challenge to technologists: Take the next STEP. January 2002.
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. May 2007.
http://www.ipc.on.ca/index.asp?navid=46&fid1=614

Incorporating Privacy into Marketing and Customer Relationship Management. Co-produced with the Canadian Marketing Association (CMA). May 2004.
http://www.ipc.on.ca/index.asp?navid=46&fid1=234

P3P and Privacy: An Update for the Privacy Community. Jointly produced with the Center for Democracy and Technology (CDT). March 2000.
http://www.ipc.on.ca/index.asp?navid=46&fid1=238

Intelligent Software Agents: Turning a Privacy Threat into a Privacy Protector. Result of a joint project of the Office of the Information and Privacy Commissioner/Ontario and the Registratierkamer, The Netherlands. April 1999.
http://www.ipc.on.ca/index.asp?navid=46&fid1=316

Privacy-Enhancing Technologies: The Path to Anonymity. Co-produced with the Dutch Registratierkamer. Volumes I and II. August 1995.
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

Privacy and Electronic Identification in the Information Age. November 1994.
http://www.ipc.on.ca/index.asp?navid=46&fid1=325

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

Telephone: (416) 326-3333
Toll-free: 1-800-387-0073
Fax: (416) 325-9195
TTY (Teletypewriter): 416-7539
Website: www.ipc.on.ca
E-mail: info@ipc.on.ca