Information
and Privacy
Commissioner/
Ontario

The New Breed of Practical Privacy: An Evolution

Ann Cavoukian, Ph.D.
Commissioner
September 2005

The New Breed of Practical Privacy: An Evolution

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

27th International Conference on Privacy and Personal Data Protection

September 14-16, 2005, Montreux, Switzerland

Good morning ladies and gentlemen. It is a great pleasure to be here today, and to once again have the opportunity of speaking to my fellow Commissioners and colleagues in the data protection community.

A great deal has changed in the last few years. Ever since the terrorist attacks of September 11th in the United States, our world has changed dramatically. *My* world as a Privacy Commissioner has certainly changed – the challenges have become far greater.

And while there may have been a temporary reprieve, the terrorist attacks of July 7 and 21 in London, England appear to have returned us to the post-9/11 world of suicide bombers, terrorist attacks, and unbridled fear. Just last week the second in command for al Queda, Mr. Al-Zawahri, claimed responsibility for the July 7th bombings. And in a recent video, al Queda threatened the west with "more catastrophes" in response to the policies of US President Bush and UK Prime Minister Tony Blair.

So, you may be wondering, why am I talking about these terrorist attacks? What does that have to do with the subject at hand? ... A great deal I think. Because, ladies and gentlemen, it will impact our activities as a data protection community, like never before, and if we do not adapt to these changes, we may lose our relevance, our impact, and ultimately, our effectiveness. While I will be focussing my talk largely on private sector initiatives, I am leading into it with the realities that we must all face these days as Commissioners – and the world of terrorism and the need for public safety forms the backdrop.

What is the one characteristic that we all share today, globally? ... We live in an increasingly security-conscious world.

Everyone appears to becoming more concerned about security and public safety – from our politicians and legislators, to our neighbours and the public at large.
The repeated terrorist attacks of the recent past have elevated the perceived threats. They have caused the leaders of numerous countries to renew their declarations of war on terrorism, with the ensuing urgency in the expansion of anti-terrorism measures and the search for new security technologies.

In my country, Canada, ever since the July 7 London attacks, there have been increasing calls for greater security measures and a commensurate acceptance of less privacy – as if such trade-offs

were inevitable. I have always taken issue with the premise that privacy and security are opposing forces, necessitating "zero-sum" trade-offs, with more security meaning less privacy. I couldn't disagree more.

In the immediate post 9/11 period, we published a paper called *Security Technologies Enabling Privacy (STEPs): Time for a Paradigm Shift*, where we shifted the focus to building privacy into security technologies – describing a process for reconciling security and privacy whenever deploying new technologies. Whereas we had previously focused exclusively on Privacy-Enhancing Technologies (PETs), now our focus shifted to marrying privacy to security, presenting them as two sides of an inseparable coin – you had to have both in order to be strongly protected.

I make every effort to explain these distinctions and identify opportunities for building privacy into security systems, but I must admit, it is an uphill battle. People seem to think that you must give up privacy for greater security. And what's worse, they seem to be willing to do that.

Our newspapers have published numerous surveys over the summer months indicating that the public is willing to accept less privacy for greater security. And regardless of the fact that these surveys have often been seriously flawed, using poor methodology and limited samples, it doesn't seem to matter. The public appears to have decided – in favour of security and public safety. My own federal Commissioner, Jennifer Stoddart, the Privacy Commissioner of Canada, has grappled admirably with numerous attacks on privacy in the form of no-fly lists, that we know very little about, and a Canadian Bill referred to as Lawful Access (which appears to be anything but lawful), which would grant law enforcement and national security agencies sweeping powers to access the personal information of Canadians at large. If passed, dramatic new online surveillance powers would be legalized, further eroding citizens' privacy while failing, in the words of one legal scholar, "to truly boost Canadians' security."

Yes, I believe that privacy is at risk as never before; consider the following:

- The need to identify individuals faster, more accurately, and more reliably;
- The need to authenticate the identities of individuals, to verify their credentials and authorizations;
- The need to check backgrounds and histories, patterns of association, to check names against watch lists and no-fly lists;
- The need to access data quickly from many sources, both public & private, and across numerous jurisdictions;
- The need to intercept communications and monitor traffic patterns of activity;
- The need to link, correlate, and sift through massive amounts of personal data, looking for patterns unknown;
- The need to share data and intelligence across different jurisdictions and domains – all in real time;
- The need to make assessments and judgements about people, that may be questionable at best, again in real or near-real time.

These growing needs for, and uses of personal information are all being justified in the name of protecting and promoting security – be it national, public, or individual.

Armed with enough personal information, public authorities firmly believe they will be able to identify and catch the terrorists, and bad guys in general, far more efficiently than ever before. We know this to be more in the realm of fiction than fact – just read the work of any respected security expert, such as Bruce Schneier. His most recent book "Beyond Fear," expresses very clearly how futile most government efforts are at expanding the net of surveillance in an effort to capture the bad guys – it simply doesn't work well, but in the process, it will cause many innocent citizens, going about their daily activities, to be detained – false positives being a fact of life.

The growing demand by public authorities for personal information parallels a similar phenomenon taking place in the private sector, where commercial interests have become fused with personalization, improved service offerings, and operating efficiency.
In many instances, and with growing frequency, the demarcation lines between public and private data stores are blurring: lawful access, secret search and seizures, purchases of databases of personal information and so forth.

The result is what I call the "New Normal," namely, surveillance on a scale and depth we've never witnessed – a function of the mushrooming collection, use and disclosure of personally identifying information, coupled with diminished oversight – a dangerous combination.

And to make matters worse, the erosion of independent oversight, be it judicial or through a data protection authority, appears to be growing, with more activity taking place under a shroud of secrecy. In my country, the Attorney General can issue a "secrecy certificate" which, being a matter of national security, cannot be reviewed by our Privacy Commissioner, nor accessed by the data subject for purposes of accuracy or correction.

And yet, whenever such concerns are raised and pleas for due process and civil liberties are made, they are often met with the type of remarks recently made by the UK Home Secretary, Charles Clarke, who last month urged European politicians to, "put the fight against terrorism above concerns for civil liberties," declaring that, "the right not to be blown up was the greatest human right of all."

During such times, a major challenge for data protection commissioners, concerned citizens and consumers, politicians, lawmakers and businesses alike, is to find ways in which to promote and ensure privacy's continued existence and viability.

How can we work together to make privacy real and tangible … both practical and beneficial? In Ontario, I talk about the need for "practical privacy," by which I am not suggesting a reduction or weakening of our expectations of privacy; no, quite the opposite. I want to ensure the long-term preservation of privacy – I want to strengthen privacy, well into the future, ever present, even in the midst of an ever-growing security-conscious world. So how do we do that?

Okay, that's the backdrop – enough doom and gloom! Let me turn now to the private sector and tell you about some positive developments that exemplify what I mean by taking a practical approach to privacy. In North America, there has been a great deal of activity relating to privacy initiatives for the business and corporate world. As you know, Canada passed its own private sector privacy legislation a number of years ago. What you also need to know is that while the United States may not have omnibus privacy legislation for the private sector, there has been a great deal of legislative activity relating to the introduction of laws to notify the public of security breaches relating to their personal information. Following on the heels of the landmark legislation in California, SB 1386, 19 states have passed new breach notification laws, with another 16 states now considering them.

Further, there is a growing privacy industry in the United States consisting of privacy professionals devoted to assisting businesses in engaging in privacy protective practices. This has blossomed into an association of a significant size – the International Association of Privacy Professionals (IAPP), which regularly meets and holds sizable conferences attended by thousands of people, Commissioners included. So it is important to recognize that in both Canada and the United States, a great deal of attention is being focussed on private sector activities in the area of privacy, which I view as a very positive development.

Let me outline three broad avenues of approach that we, in Ontario, are taking:

1. Expand the application of Fair Information Practices beyond the existing front-end focus (based essentially on notice and consent), to a more comprehensive application of privacy principles, shifting greater focus on the protection and integrity of personal data. I refer to this as adopting robust information management practices or RIM, and I will be illustrating this point in its application to identity theft;

2. Greatly improve communication and engagement with data subjects and the public on a day-to-day basis – I see our relevance and accessibility as Commissioners being key here; I will illustrate this point with our use of short notices;

3. Build in privacy at the outset – at the earliest stage possible – into technology and IT systems, building upon a commonly accepted global privacy standard, which I personally believe, we can develop together.

I will briefly describe each of these approaches and illustrate them with examples from the work that my office has done.

1. Adopt Robust RIM – Responsible Information Management Practices: TRUST, BUT VERIFY

With so much personal information coursing through the veins of our information age, the time has come for a broader and deeper implementation of Fair Information Practices by all organizations. I will be discussing this in the context of the recent epidemic of identity theft that has swept across North America.

Personal information has become both a significant asset and a liability to its custodians. When managed well, organizations earn the trust of their clients. When managed poorly, trust and confidence quickly erode.

I believe that the data protection community has a critical role to play in capitalizing on opportunities to promote the full and verifiable adoption of Fair Information Practices. Data privacy is a perspective and an approach to information management that is distinct from security. Data privacy is much more comprehensive, subsuming a broader set of protections than security alone.

And we may have an excellent opportunity right now to engage stakeholders. In light of the numerous security breaches reported this year, especially in the United States and Canada, we may be witnessing a perfect privacy storm, a "teachable moment," for all parties involved.

The public and lawmakers are waking up to the enormous negative impacts on innocent members of the public of poor information management practices – one of the major ones being identity theft.

There is growing sentiment to introduce new restrictions on certain information practices, impose new obligations upon information custodians, and to vest data subjects with greater choice, access, and correction rights.

New bills, legislation and regulations are being proposed across the United States, intended to curb the excesses of abuses to privacy. In Canada, a federal-provincial public consultation is now taking place, lead by the Consumer Measures Committee, exploring options to amend our federal and provincial laws to curb identity theft.

There are many opportunities here to ensure that a robust interpretation of Fair Information Practices is included, not only in proposed laws and regulations, but in standard business practices. And the demand for robust information management practices is now being driven in part by the growing awareness of privacy breaches.

In Ontario, I have been calling for private-sector privacy legislation at the provincial level, which would include a mandatory breach notification requirement, as does our new health privacy law, which entered into force last year. This would represent, in my view, the next generation of privacy laws.

Of course, most organizations shouldn't need more encouragement to be proactive and to adopt stronger, more verifiable, privacy practices. Earning the trust of customers – not to mention supply chain partners and oversight agencies – will demand it.

We're giving those incentives a helpful nudge by publishing a paper on identity theft that swings the spotlight of responsibility upon businesses to minimize identity theft by adopting a comprehensive data privacy program. The paper offers advice on how to apply fair information practices –throughout the entire data lifecycle, with a strong emphasis on encrypting databases

containing massive amounts of personal information. It also suggests that we stop blaming the victim and expecting them to somehow single-handedly curb the rising tide of identity theft – they cannot.

Businesses will need guidance in developing and implementing effective privacy policies. Privacy Commissioners can help by offering useful tools and guidance for businesses to follow.

We think the time is ripe for such materials and guidance to be codified into best practices, and for privacy practitioners to be recognized as a distinct profession, with its own unique corpus of knowledge required, perhaps with recognized credentials.

At the same time, there is a growing need for privacy audit and verification standards and services, for stronger evidence of privacy enforcement and accountability. We as Commissioners can lead by assisting in these efforts, further demonstrating our ongoing relevance.

2. SHORT NOTICES: Make Notices Shorter, More Accessible, and Easier to Understand

If there is one thing that all privacy commissioners are mandated to do, and are good at doing, it is to educate, facilitate, and otherwise make stakeholders aware of their privacy rights and obligations.

If privacy is to be preserved in this security-conscious information age, a sufficiently broad base of the public needs to be engaged in this issue. Opportunities for meaningful dialogue with organizations about their privacy policies should be pursued.

The problem is, how to do this? How <u>not</u> to do it is by using lengthy, complex, unreadable privacy policies and notices, immersed in legalese with a lack of guidance, lack of standardization, a fear of liability, and an abundance of weasel words. The end result of such an exercise is highly ineffective as a communications tool, and leaves the public cold. It discourages citizens and customers from reading, let alone understanding and exercising effective, informed choices.

So, someone comes along with the bright idea to develop "Short Notices" or multi-tiered notices, consisting of an initial short notice, followed by additional explanatory pages.

That someone was Marty Abrams, of the Center for Information Policy Leadership, at Hunton & Williams, who can be credited with the idea for developing a short notice template, which eventually lead to The Berlin Memorandum Resolution adopted at the 2003 Data Commissioners' Conference in Australia.

The key idea was to develop standardized, comparable notices, that are concise, written in plain language (not legalese), are easy-to-understand, and layered so that additional information can be provided to interested parties.

To describe this as a better way to communicate – by involving the data subject, obtaining consumer consent more effectively, and engaging people in the privacy process by giving them something they can actually understand, is an understatement. The value of short notices cannot be over-stated.
This is not to not suggest that short notices are a substitute for carefully constructed, detailed policies and procedures; yet, they are highly suitable and appropriate in numerous contexts, especially if you are trying to reach the public and engage them in a meaningful exchange. To lose the interest of the data subject from the outset is to lose their understanding of the issues and ultimately, their interest in an understanding of their rights – in their privacy.

So we decided to develop short notices in a new privacy law introduced in Ontario last year, the Personal Health Information Privacy Act, or PHIPA. Its scope is extensive, covering all healthcare providers, doctors' offices, health facilities, laboratories, testing facilities, etc.

We worked closely with our legal and health care professionals to develop a standardized set of language and a vocabulary to include in the notices, along with the appropriate presentation of choices regarding the privacy options available to those seeking care.

We developed three sets of posters and accompanying brochures: one set for use in hospitals, one for doctors' offices, and one for health care facilities such as nursing homes and homes for the aged. The results were a resounding success – demand for these short notice packages has been very high! In the first two months – July and August – we have sent out just under 300,000 short notice brochures and posters, in response to requests received from those covered by the law.

I am delighted with the outcome of these short notices but I want to emphasize that it is very important to involve your legal professional association, in my case, the Ontario Bar Association – their buy-in was very important to the success of this project. The most important feature of the project was that it demonstrated our usefulness to the community impacted by this new health privacy legislation. We saved them the work of developing these notices and brochures, and in so doing, we made sure we developed tools that would be helpful and easy-to-understand by patients and practitioners, making it more likely that they will actually be read and understood.

We have copies of these packages available to any of you who might be interested in them.

3. ONE GLOBAL PRIVACY STANDARD

There are many demonstrable benefits to being proactive – to building in privacy from the outset. The role and stature of Chief Privacy Officers is growing. We are also seeing the emergence of new, multidisciplinary information management professionals, needed to make privacy real and operational: privacy architects; privacy designers and design specification writers, to name a few.

My office is involved in multiple ways to help ensure that bad design choices are ruled out at the beginning, wherever possible.

Perhaps our greatest privacy success as commissioners comes, not from punishing privacy transgressors, but in helping to deter poor architectural design from the start, thereby helping to avoid a potential "Privacy Chernobyl."

There are numerous projects currently planned or underway that hold forth significant implications for privacy. As Commissioners, we are all asked to comment on proposals for identity cards, e-government portals, passenger profiling/screening, lawful access initiatives, as well as the use of specific technologies such as RFID chips and biometrics.

We know that information technologies are privacy-agnostic, but that the devil is in the detail. Decisions made today will have long-term impacts. We also know that many technologies can be privacy enhancing, if they are designed and deployed properly.

So, how do we encourage the research, development and design of privacy-enabling technologies? Ideally, there would exist a unified, common vocabulary for describing and measuring privacy and its attributes in information systems.

The PETTEP project started several years ago to test the functionality of privacy claims about a particular technology or system. The framework was broad enough to handle a wide variety of privacy claims and assertions about information technologies and systems.

But there was one problem – currently, there is no commonly accepted international privacy standard – no single, global privacy standard.

So upon reflection, it occurred to me that to begin with, what we needed to do was return to first principles: there is a more pressing need to harmonize Fair Information Practices into a single Global Privacy Standard (GPS), after which we would be in an ideal position to provide guidance on how such a standard could be interpreted and implemented in privacy-enhancing technologies and IT systems.

On Friday morning (September 16), I will be chairing an international committee of Privacy and Data Protection Commissioners, formerly referred to as the Wroclaw Foundation, to review leading fair information practices presently in use around the world, in an attempt to harmonize those practices into a single common set of Fair Information Practices that we, as a data protection community, can support. If we could accomplish this goal, then it would enable us to speak with one voice, which I believe, would strengthen our global presence.

My office has already conducted some of the preliminary work by conducting what I refer to as a "Gap Analysis." We have begun the process of comparing the leading privacy practices and codes from around the world, comparing their various attributes and the scope of the privacy principles enumerated therein – attempting to identity the strengths and weaknesses in the six codes examined. I will be tabling and presenting our Gap Analysis on Friday, for the consideration of the Board members, and I invite any interested Commissioners to join us at 8:00 a.m. on Friday.

Ultimately, we may wish to work with the standards bodies such as ISO's Committee on Consumer Policy (COPOLCO), who are eager to develop a privacy checklist and evaluation framework for assessing the privacy impacts of new technical standards and systems, as well as with other standards bodies that are interested in building upon our global privacy standard. But they will have to wait. We will only consider establishing contact with the standards bodies once our initial work of harmonizing the principles in the various codes has been completed. First, we must develop a harmonized set of fair information practices that builds on the strengths of existing codes – that is my objective. I would be happy to discuss this further with anyone who is interested.

CONCLUSION

Everywhere today, information privacy is at risk, eroded by the twin imperatives of stronger security and greater efficiencies – and the sheer availability of mountains of personal data – perhaps now approximating, on average, one terabyte per person on earth.

The challenge for data protection commissioners and the international privacy community is to act together in an effective and meaningful way to protect and promote privacy.

I have argued that, in order for there to be "One World" of privacy, we need to take practical steps and engage in measures that will ensure that privacy is:
(1) effected through robust and verifiable responsible information management practices;
(2) communicated to data subjects to allow engagement and informed choice via short notices;
(3) built into technologies at an early stage, reflecting a single, global privacy standard;

At all times, my emphasis has been focused on practical, real-world solutions, with demonstrable benefits for data subjects.

Privacy cannot appear to be a luxury right or a conceptual abstraction. We must remain current and relevant, ensuring that the importance of privacy is understood and embedded into the fabric of everyday life, hence my use of the term, "practical privacy," – it's a work in progress, which will hopefully continue to evolve.

– Thank you very much –