Information
and Privacy
Commissioner /
Ontario

Privacy Protection is Good Business

a presentation by

Assistant Commissioner Tom Mitchinson

to the

Sarnia Lambton Chamber of Commerce

May 16, 2003

Information and Privacy Commissioner/Ontario

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

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

This publication is also available on the IPC website.

Privacy Protection is Good Business

Thank you very much for the kind introduction.

It is a real pleasure to be in Sarnia to talk to you about an often overlooked but increasingly critical business issue – privacy. The *Wall Street Journal* has tagged privacy as the No. 1 issue of the 21st century.

Many of you may be wondering what relevancy privacy has for your business. After all, protecting privacy is a government issue – **right**. I mean, why spend money protecting the privacy of your clients and customers when what you really want is access to **more** information – on the habits and needs of existing and potential customers.

Well, the reality is, protecting privacy is a bottom-line business issue for virtually all companies in Canada. Do it well and it will help you prosper. Do it poorly and you will pay a steep price.

Today's customers are demanding that companies keep their personal information private. Failure to do so can seriously damage your reputation. Respecting your customers' privacy is quite simply good business. It fosters trust and builds consumer confidence. It strengthens brand recognition, increases customer loyalty and, ultimately, delivers competitive advantage.

We have all read or heard of far too many cases recently where business records or files have been stolen or hacked into – and the personal files of millions of people compromised. Each of these individuals is subject to *identity theft* simply because the organization holding this information was not able to protect it from thieves.

The real news story on these cases will be heard eight to twelve months from now when an unfortunate number of these customers find themselves bankrupt or worse – because their financial or legal records were stolen. According to police, it often takes this long before people realize their identity has been stolen and used by someone else.

The companies that allow this to happen to their customers suffer significant blows to their reputations and the confidence of their customers, shareholders and investors. Privacy has now become an essential part of any business's "competitive edge."

A recent survey found that Canadians have very little trust in the desire and ability of companies to protect the privacy of their personal information. Online consumer sites scored the worst, while banks came out on top.

When asked who they trusted the most with their personal information, 36 per cent of respondents said banks, 27 per cent cited their employers, and 16 per cent answered the government. Online consumer sites were cited by only one per cent of the respondents.

As Dina Palozzi, Chief Privacy Officer with the BMO Financial Group, notes:

> In any business, privacy of personal information is important; in banking, it is essential. We take our responsibility to respect and protect the privacy and confidentiality of our clients' personal information very seriously. [It is] our belief that trust is a key factor in securing and building lasting client relationships.

Banks seem to get it. Your challenge, and ours as well, is to ensure that all components of the business sector step up to the privacy challenge.

Before I go further, I'll step back for minute and outline the role of the Information and Privacy Commissioner of Ontario.

The Information and Privacy Commissioner, Ann Cavoukian – like the Ombudsman and Provincial Auditor – is a statutory officer of Ontario's legislative assembly. She and her office operate at arms length from government and serve a number of oversight and advisory functions.

The Office of the Commissioner (commonly known as the IPC) provides an independent review of government decisions and practices regarding access and privacy in the public sector. We help to safeguard the rights established under Ontario's access and privacy statutes – the *Freedom of Information and Protection of Privacy Act*, which has been in force since 1988 and applies to provincial ministries and agencies; and the *Municipal Freedom of Information and Protection of Privacy Act*, which followed in 1991 and applies to municipalities and other local bodies such as school boards and police services.

As Assistant Commissioner, I am primarily involved in the access side of our work. In this area, the IPC functions as an administrative tribunal, hearing appeals from individuals or organizations when a provincial or municipal government body has denied access to information. You might know these by the term "freedom of information" or "FOI appeals."

The two statutes provide a right of access to information held by government organizations. If you submit a request for access to government-held records and the government department decides not to provide you with everything you have asked for – you can appeal that decision to the IPC.

Ontario's public sector legislation also regulates the collection, use and disclosure of personal information. We investigate complaints by individuals who feel that their privacy has been breached by a provincial or municipal government organization.

In addition, the Commissioner has a large education mandate. The IPC:

- advises on proposed government policy and legislation;
- conducts research on access and privacy issues; and
- delivers programs to educate the public about access and privacy matters.

The later two objectives look at the broader issues of privacy and access and – particularly on the privacy-side – go well beyond the public sector boundary.

We are in Sarnia as part of our *Reaching Out to Ontario* public education program. A team from the IPC visits four or five communities in Ontario every year. We meet with local FOI and privacy professionals, staff from legal aid clinics, education officials and other users of our access and privacy laws – as well as with business leaders, like those of you here today.

We had a very busy day yesterday. Our team met with area school boards, legal clinics, municipal governments and the local media. We also tried something different by hosting an information booth at the Lambton Mall throughout the day yesterday to try and "reach out" to as many people as possible. With a steady stream of people stopping by to ask questions and share experiences, we think it was a great success.

As some of you will know, Ontario has been working on legislation that would regulate the collection, use and disclosure of personal information by businesses and other private sector organizations. The draft bill names Ontario's Information and Privacy Commissioner as the oversight body.

Unfortunately, this legislation did not make it through the provincial legislature before the close of the last session. Given the prospect of a provincial election coming up soon, there is no current timetable for reintroducing the legislation.

At first blush, a number of you may think this is a good thing and be relieved that you don't have to worry about it. However, a lack of an Ontario bill doesn't mean that there are no laws governing privacy.

Federal privacy legislation was enacted in 2001 that governs federally regulated industries in the country – such as banking, telecommunications, cable service and inter-provincial transportation.

On January first, 2004, the *Personal Information Protection and Electronic Documents Act* (often referred to as PIPEDA) will be extended to cover all private sector companies in Canada. The *Act* encouraged – and expected – all provinces to draft their own substantially similar privacy laws.

Without provincial legislation, the federal laws will apply. And if you have any questions or concerns you must deal with Ottawa – not Queen's Park – unless substantial pressure is placed upon the provincial government to move a made-in-Ontario law forward.

Either way, the reality is, businesses – large and small – have a little more than seven months to get their policies and systems in place to ensure the information about their customers and suppliers is properly managed and secured.

So what is privacy?

In 1890, U.S. Supreme Court Justices Brandeis and Warren wrote a groundbreaking essay entitled *The Right to Privacy*. In it, they defined privacy as "the right to be left alone."

This definition encompasses, I think, the two main planks that are most relevant to the current discussion of privacy: control of physical spaces, and control over your personal information.

Most privacy protection regimes are mainly concerned with this second aspect of privacy – control over personal information.

But the two aspects often overlap. Direct marketing is a good example. Because the transfer or sale of personal information can lead to things like unsolicited telephone marketing, informational privacy issues can have a direct impact on our physical space and a sense that someone is using your personal information to "invade" your homes.

In a 2001 Ekos poll commissioned by the Public Interest Advocacy Centre on *Business Usage of Consumer Information for Direct Marketing*, Canadians expressed high levels of concern about unsolicited direct marketing, particularly telemarketing.

85 per cent received unsolicited advertising material during the previous month, and 74 per cent reported high or moderate concern about this. Telemarketing is a particular sore point, with 61 per cent wanting no telemarketing calls to their household – even if that means they miss out on a really good opportunity.

Ekos also found "... a strong consensus when it comes to whether or not companies should ask for permission before they use an individual's personal information for marketing purposes," with 82 per cent of respondents believing they should.

The first attempts to define the parameters for ensuring the privacy of personal information were laid out in a set of Guidelines adopted by the Organisation of Economic Co-operation and Development in 1980. In 1996, the Canadian Standards Association used these Guidelines as the basis for its Model Code for voluntary adoption by Canadian businesses.

Canada is certainly not alone in its commitment to effective regulation of privacy. In 1995, the European Union enacted a Data Protection Directive that restricts transborder flows of personal information to countries that do not have adequate privacy protection in place. The persuasive power of this Directive has been a significant force in shaping Canada's private sector privacy legislation.

The CSA Model Code consists of 10 privacy principles, often referred to as *Fair Information Practices*. Although perhaps not anticipated back in 1996 when the CSA Code was issued, it turned out to be an extremely important document, since it was eventually incorporated into the federal government's private sector privacy law, the *Personal Information Protection and Electronic Documents Act*, mentioned earlier.

I'd like to highlight a few of the CSA privacy principles I think are most important for this audience to be aware of:

Identifying Purposes: making sure that customers know up-front exactly why their personal information is being collected and how that information is going to be used or disclosed.

Consent: getting consent for the collection of personal information, as well as consent for any subsequent or secondary use or disclosure of this information.

Limiting Collection: limiting the collection of personal information to that which is necessary to fulfill the specified purpose.

Limiting Use, Disclosure, Retention: if personal information has been collected for a specified purpose, with the consent of the customer, that information should not be used for another purpose, except with the consent of the customer, or as permitted by law.

Safeguards: ensuring that personal information in an organization's possession is kept safe from unauthorized access.

Individual Access: letting people see what information has been gathered about them, and giving them the opportunity to correct it.

Now the area where the impacts of privacy protection – or I guess the lack of privacy – has had the most impact on business is the evolution of the Internet as an economic vehicle. E-commerce has not come close to fulfilling its promise of radically changing the way business is conducted.

In 1998, *Business Week* made this statement about privacy and the business potential of the Internet. (Cited in accompanying slide.)

These are pretty strong words, especially for a publication like *Business Week*.

As you can see, this promise has faded over the years.

And there's no doubt that changing attitudes to privacy have taken their toll in very real economic terms; the numbers don't lie. Projections for the development of e-commerce have steadily been decreasing.

In the U.S., according to the Department of Commerce Census Bureau, only one per cent of total sales resulted from online transactions – that's $32.6 billion American dollars, for the entire year – small change considering total retail sales for just the fourth quarter alone was nearly $861 billion. And business-to-business transactions accounted for 94 per cent of all e-commerce activity.

In Canada, according to Statistics Canada, the total value of customer orders sold over the Internet was $10.4 billion in 2001 – only 0.5 per cent of revenues. Again, what we are seeing here is e-commerce not making any real dent in consumers buying practices – much of this attributable to a lack of comfort in transmitting private information across the cyber highway.

As we see in the assessment done by Forrester, privacy fears cost big money.

Another recent study – the UCLA Internet Report 2001: Surveying the Digital Future – found:

- more than one-half of Internet users (56.5 per cent) and nearly three-quarters (74.5 per cent) of non-users believed that "people who go online put their privacy at risk."

Nearly all respondents (94.5 per cent) report some level of concern about privacy if they buy online.

And the issue of privacy continues to raise barriers to online sales – especially among infrequent purchasers:

- nearly all users with less than one year of experience (98.6 per cent) express some concern about credit card information when they buy online.

In 2001, Forrester thought lack of solid privacy and security practices could cost retailers $15 billion over the next few years.

Jupiter Research has now increased that number to $25 billion – that's a serious amount of money to miss out on.

What can and should business do to win this confidence battle?

No less a source that Alan Greenspan has said that the best means to counter technology's erosion of privacy is technology itself. (See slide.)

When privacy is considered to be an information management tool – an essential strategic resource, not a tool of regulatory compliance – it can become a key business differentiator for companies.

Like most other aspects of business, effective planning is key to safeguarding your clients' privacy. The most important thing to consider when setting up technological safeguards for privacy is that it is far easier to build in privacy protections at the outset, than it is to try to retrofit solutions after the fact.

But remember, in addressing both privacy and security, the deployment of technology is not the end of the story. Remember that a large number of security breaches do not come from the outside – but rather from individuals within an organization. Often it is just a matter of poor or incomplete policy, or simply a lack of training.

Technology is definitely not the total solution to your privacy challenge. The best security technology may protect a system that collects and uses personal information in a manner that is completely privacy-intrusive – and in direct conflict with the expectations and desires of your customers and clients.

This picture (see slide) is a good example of how you can have perfect security (imagine the bird is in a six-inch thick bullet-proof glass cage – with appropriate air holes), but no privacy.

What is needed is the development of a privacy protective corporate culture. It has to become second nature to consider the privacy concerns of clients, not an afterthought. Everyone has to be involved, from the CIO down through the legal department and the systems department, to the customer service representatives.

At the IPC, we have worked to build practical tools to help businesses assess their ability to safeguard privacy. With the help of PricewaterhouseCoopers and Guardent, we developed the IPC's *Privacy Diagnostic Tool* as a way to help businesses assess their readiness to grapple with privacy protection measures.

The PDT is designed to help take a company's "privacy pulse." It's not based on any one piece of legislation, and it's not geared towards any one industry. It is grounded on the set of fair information practices we have been talking about this morning. The PDT takes a company through sets of questions that will help it determine whether its business practices are protective of its customers' privacy – or actually a threat to it.

Once you get to the end of the series of questions, the PDT will generate a printed report, to let the company know what privacy areas it is strong in, and where it still needs work.

No one else sees the report. It's for the company's information and action, and should help it prepare for the new privacy legislation.

As I touched on briefly a moment ago, effective oversight of privacy issues is all about educating organizations regarding their responsibilities – and sharing expertise on how to best discharge these new duties. We have had a great deal of success in following a collaborative and non-confrontational approach with public sector organizations – and we think that same approach would be most effective with business as well.

Occasionally – and some of you may be aware of examples from media reports of our work over the years – we need to get tough. It is important that the law provide the teeth necessary for effective oversight. But, while a stick is necessary in order to deal with the exception, there is no doubt in our minds that a carrot is by far the more effective approach when dealing with privacy.

In addition to the *Privacy Diagnostic Tool*, we have also created a number of other tools and checklists to help business get ready for the privacy challenge. Here are some of the key steps we believe need to be undertaken. (See slide.)

As business leaders, it is important that you understand the costs and benefits of privacy issues to your business. Whether operating under a federal law, or at some point under a made-in-Ontario law, it is vital that all organizations understand their legal obligations and requirements – as well as their own business needs related to privacy.

This understanding is critical so that a company can establish the appropriate policies and procedures to implement its own privacy regime. Some larger organizations may want to consider appointing a Chief Privacy Officer, with dedicated responsibilities for ensuring that personal information management processes are soundly designed and effectively managed.

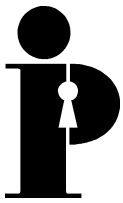
However, at the end of the day, the real measure of success for an organization will be the extent to which it has been able to move beyond simply complying with a set of rules, and to actually embrace a culture of privacy within its organization. The proper management of personal information must become second nature in order to be truly and consistently effective.

I'll close with what I think are two interesting and thought-provoking quotes. The first is from Forrester Research in one of its 2001 reports. (See slide.)

The second is from one of the world's foremost experts on privacy protection – Ontario's Information and Privacy Commissioner, Ann Cavoukian. (See slide.)

Privacy is in its infancy as a public policy issue, and the tough news is that we all have a lot of work ahead of us in adjusting to the new realities and expectations of members of the public and our customers. However, the easy part is that good privacy is, to a large extent, really just good common sense. The principles and values that underlie privacy are simple to understand, easy to accept, and relatively straightforward to implement. And the sooner you embrace the new more privacy-focused world, the better it will be for you and your business.

Thank you for having me here this morning, and giving me the opportunity to share some ideas with you.



Information and Privacy Commissioner/Ontario

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

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