http://www.privcom.gc.ca/speech/02_05_a_010326_2_e.asp

Address by the Privacy Commissioner of Canada delivered to the Privacy Lecture Series

March 26, 2001 Toronto, Ontario
George Radwanski Privacy Commissioner of Canada

I'm very pleased to have this opportunity to meet with you. I'm going to try to speak relatively briefly, share some thoughts with you and then leave as much time as possible for questions and give-and-take.

Let me begin by telling you a bit about my role in the privacy landscape.

As the Privacy Commissioner of Canada, I am an officer of Parliament, appointed for a seven-year term to be the independent guardian and champion of the privacy rights of Canadians.

The Privacy Commissioner of Canada doesn't work for, or report to, the government. I work for and report directly to the people of Canada, through our national Parliament.

I am mandated to oversee and enforce two critical pieces of national privacy legislation: the Privacy Act that governs the federal public sector, and the new Personal Information Protection and Electronic Documents Act, that began coming into effect in January and that for the first time gives Canadians clear privacy rights in their dealings with private sector organizations.

I also have a legislative mandate to raise public awareness and understanding about everything pertaining to privacy, and to research privacy issues and provide independent advice to Parliament and the government.

I know that there are a lot of people out there who think that people like me, and the legislative protections that we enforce, aren't worth very much when it comes to protecting privacy. They say that you're better of relying on technology, using it yourself to protect yourself.

But I have problems with this view. And to explain what those problems are, I want to talk a little more about the relationship between privacy and technology.

Before I came here, I looked over the calendar of lectures for this series, and read about some of the sessions you've already had, and some that are scheduled. You've had people talking to you about cybercrime and about wireless privacy. You'll be hearing about computer crime and protecting computer databases. I also noticed a number of

"privacy headlines," dealing with subjects like biometrics, electronic payment systems, and tracking of e-mail through javascripts. This technological focus doesn't surprise me, because that tends to be how privacy is viewed. Ask people what privacy is about, how privacy is threatened, and the chances are good that they'll l talk to you about the Internet—about cookies and web bugs, about tracking and profiling of web-surfers, about the security or insecurity of data on the Internet, about the confidentiality and security risks of e-mail.

They're talking about new technology—but the idea that technology threatens privacy isn't new at all.

Much of our modern notion of privacy, the threats to it, and the need to protect it, grew out of past encounters with new technology.

In fact, one way to look at the development of the modern understanding of privacy and its protection is to see it in the context of technological developments.

It's customary to view our modern notion of privacy rights as starting with the article that Samuel Warren and Louis D. Brandeis published in 1890 in the Harvard Law Review, entitled simply "The Right To Privacy." Warren and Brandeis were responding to, as they put it, "recent inventions and business methods." The business method was the popular press, and the most striking of the recent inventions—the technology—was the instantaneous photograph. Suddenly, it was easy to take spontaneous, unposed, and often uninvited photos of people—which Warren and Brandeis denounced as "invad[ing] the sacred precincts of private and domestic life"—and to show the results to a large, literate, curious, and gossipy audience. This new technology was so insulting, so threatening, to Warren and Brandeis that it led them to think about exactly what it was that was being invaded, being taken from them, in such a new way. They defined it, as "the right to be let alone"—a definition of privacy that's far too limited in today's context, but that is still easily understood, and widely accepted.

Another major step in theorizing privacy came in the late 1960s and early 1970s, with, for example, Alan Westin's Privacy and Freedom, published in 1967, and the Canadian government's own in-depth study leading to the 1972 report Privacy and Computers. Here again, we can see the technological threat to privacy as the impetus. Westin referred to "telephone tapping, electronic eavesdropping, hidden television-eye monitoring, 'truth measurement' by polygraphic devices, personality testing for personnel selection, and"—the thing we've come to see in retrospect as the most important development—"growing dossiers of personal data about millions of citizens." The development of these data banks and the growing use of computers that shared, matched, and mined them was the focus of the Canadian government's study. And, it was also, it seems to me, the most important context for Westin's work. It was this

phase that saw theorists trying to define privacy in new and more expansive ways—definitions that were less terse and maybe less elegant than the formulation used by Warren and Brandeis, but better suited to the more complex challenges privacy had begun to face. My own definition of privacy—the right to control access to one's person and to information about oneself—is to some degree inspired by the work that was done in this period. The third wave of interest in privacy really hit in the 1990s, with such force that we're hard put to name a principal theorist or popularizer—because there are just so many of them. Interest in privacy, writings about it, theories as to how it should be protected—they've all just exploded in the last few years. The big technology story behind this was, of course, the Internet. And not just the Internet-because that had been around for a while-but widespread individual use of the Internet, with people all over the globe tapping into the Net from their personal computers...and in the process being identified, tracked, recorded, classified, and analyzed as they surfed.

So that's three waves of interest in privacy, reflecting three distinct phases in the development of technology. With privacy conceived in terms of technology, it's natural enough to look to technology as the means to protect privacy. And so we have privacy-enhancing technologies like encryption and anonymization—technological solutions to a technological problem.

But I don't have a whole lot of enthusiasm for technological solutions. I know the arguments for them—that technology develops faster than legislation can keep up; that enforcement of legislation just ends up being more surveillance and control; that government is itself the biggest threat to your privacy, and not the party you should invite to protect it.

But no matter how well things like encryption and anonymization work, and how easy they become to use, these solutions are basically a kind of "technological opt-out." You're familiar with the opt-out/opt-in distinction, I'm sure. It's well-known terrain to anyone who's fought privacy battles, or even just observed them. Someone who wants to collect, use, or disclose our personal information gives us the option to say we don't want them to. In the off-line world, it's often a matter of calling or writing, for example to the Canadian Marketing Association, to get yourself onto a "Do Not Mail/Do Not Call" list. It may be as simple as checking off a box that says, "If you do not want us to send you this useful information from time to time,...." If we haven't taken them up on this offer to opt out, they proceed as though they have our consent. Most privacy advocates, myself included, consider opt-out to be pretty poor privacy. Consent is a fundamental principle of privacy protection, maybe the fundamental principle. Opt-out is basically a very weak form of consent—you are presumed to consent unless you indicate otherwise. I share the view that this puts the responsibility on the wrong party. Someone wanting to collect, use, or disclose your personal information should be required to get your active consent—invite you to opt in. Opt-out is one of those things that works better in

theory than in practice. Your ability to opt out assumes that you know there's something going on that you can opt out of, that you know you have the right to opt out, and that you know how to opt out.

It also assumes that opting out is in fact a valid, realistic option.

Those assumptions might work for the informed, patient, literate, aware consumer advocate. They don't work particularly well as the basis for protecting the privacy of all of the people, all of the time. Opt-out simply does not extend the privacy net as widely as opt-in—and that, of course, is why so many marketers and information-collectors prefer it.

Encryption and anonymization, and privacy-enhancing technologies generally, take all these shortcomings of opt-out in the off-line world ... and add a whole new layer of problems. Now it's not enough that you know what's going on, and that you know you can opt out if you want.

Now you have to have, not just literacy, patience, and determination, but also a certain level—in some cases a high level—of technological sophistication.

And you have to have money—while some of these technologies are made available as "freeware" on the Internet, the hard reality is that the makers of privacy-enhancing technologies are not in business for their health.

Is this how we respect and protect a fundamental right?

It's common, in talking of privacy protection, to use the analogy of the way we physically protect ourselves and our property. In fact, the most common icon depicting privacy-enhancing technology, in advertising and on our desktop computers, is a padlock. You can protect your property against crooks with locks and alarm systems-just as you can protect yourself against muggers by choosing carefully where and when you venture into the street. But, as a society, we don't leave it at that. You have some responsibility to protect yourself, sure. But if you can't afford the best locks or a state-of-the-art alarm system, or you don't know how to use them, or if they don't work because the crooks get smarter—we don't shrug and say, "Tough luck." You should protect yourself from crooks, but whether you do or not, we don't say that crooks are entitled to try to break through your defences—and if they succeed, too bad for you. You'll have to protect yourself better next time. The reason is simple enough: theft and mugging are considered to be acts against society, not just against you as an individual. Your right to be secure in your person and your property is not just your individual right: it's a social right.

Society as a whole—not just you as an individual—is considered to benefit from it. The law provides sanctions and protections, and the state provides resources to ensure that these social rights are protected. I don't mean by using this analogy to get you thinking of marketers and data miners as crooks and muggers. My point is simply that we should not accord privacy less importance than we give to property and security of the person. Privacy, like property and personal security, is important to society, not just to individuals.

Without privacy, there is no real freedom. In fact, many have suggested that privacy is the right from which all others flow – freedom of speech, freedom of association, freedom of choice, any freedom you can name.

That's why privacy is recognized as a fundamental human right in the United Nations Declaration of Human Rights. And it's why lack of real privacy is a distinguishing characteristic of so many totalitarian societies.

So anonymization and encryption and privacy-enhancing technologies in general may useful and important, but they are still technological opt-out.

And my position is that, in cyberspace as in the "real world", we shouldn't have to opt out. The default setting should be that our privacy is respected.

Then how did we get to this focus on technology as a solution to the problem of protecting privacy? It seems to me that we end up focusing on technological solutions if we envisage privacy as a technological problem. If you conceive of privacy as a problem of technology, it's natural enough to look to technology for solutions. But I see privacy a bit differently. I see privacy as a social issue; I see the threats to privacy as part and parcel of larger social developments.

Let's look again at the technological context for the three waves of privacy protection that I talked about earlier.

In 1890, when Warren and Brandeis were defending privacy against the threat of new technology in the form of the photo, they were not dealing with a simple technological phenomenon. An unposed, unsolicited photograph itself is neutral - what concerned Warren and Brandeis was what was done with it, in the "gossip press" and in commercial advertising.

However much they can be credited with theorizing privacy, the fact is that Warren and Brandeis were rather more interested in protecting the privileges of a patrician class against a growing middle class that was starting to flex its muscles politically and culturally.

As I noted earlier, it's common to look at the work done on privacy in the late 1960s and early 1970s, and see the influence of computers and databases. But in my view what was more significant was the social context of the 1960s: the rise of the welfare state, the increasing need to "know things" about the populace in order to design and deliver social programs, and, most important, the interest at every level of society in individual freedom and self-determination—which cannot be achieved without privacy.

And then the third wave, in the 1990s. Yes, it was the Internet, but it was more than that. What made the Internet a privacy battleground was not the technology on which it was based. It was the change in the way that sellers were looking at customers: the development of "customer relationship management"—the recognition that keeping customers required knowing them, and that getting new customers required finding out about them. This was not a technological phenomenon. Cookies—a word which for privacy advocates packs more meaning into two syllables than "Bastille" does for the French—only became a privacy issue when advertisers and commercial sites realized their value in tracking individuals for commercial purposes. In other words, it's not the cookie, it's the use of the cookie.

I want to come back to another aspect of the technological opt-out, and the technological conception of privacy on which it's based.

I said earlier that consent is the fundamental principle on which privacy protection is based. That, in fact, was only part of the story.

Consent is fundamental to privacy, and, in a certain conception of society, consent works as the basis on which privacy is protected.

The problem is with that conception of society—a society made up of independent, autonomous individuals, all contracting with each other, all free to apply the best of their abilities to working out the best deal with everyone else. I know that this vision of society is dear to libertarians, but I don't think it does much for an understanding of what happens in the real world. What it overlooks is the reality of power imbalances. Most people, in most situations, don't have the option of not consenting. If a credit card issuer or a telephone company demands information from you as a condition of service, your "consent" is pretty much a formality.

You can refuse to consent to provide the information required for a telephone or a credit card—and then see how much of modern life you can participate in. You can't afford to say no, any more than a low-income homemaker can afford to turn down the discounts that come with supermarket loyalty programs. That's why we need more than opt-out—technological or otherwise. That's where legislation comes in. The key element that a

statute like the Personal Information Protection and Electronic Documents Act brings to the mix—the thing that no technology, no self-reliance, no market mechanism can bring—is reasonable limitation on the collection, use, and disclosure of information. It's only through legislation that we can do this. Without it, in the real world of imperfect markets and unequal partners, where withholding consent is rarely a realistic option, consent simply becomes a condition you have to fulfill if you want to sit at the table. The statutory restriction of the collection, use, and disclosure of information to "purposes that a reasonable person would consider appropriate in the circumstances" is what prevents consent from being reduced to a mere empty formality.

That brings me to my concluding comment. I've often said that we are at a crossroads.

I believe that privacy will be the defining issue of this new decade. How we deal with privacy now will have profound implications for the future we leave for our children and grandchildren, for the relationship they have with each other, with the rest of society, with the state. To deal with the challenge facing us, to ensure that real privacy is strengthened, preserved, and protected, we need more than technological solutions. We need actively engaged citizens. We need privacy advocates. And we need legislation with teeth—Privacy Commissioners with the will to chomp down with those teeth if and when necessary—to protect privacy in the real world.