

Finding the Balance between Privacy and Security

Notes for an address to the Annual Conference
of the Canadian Access and Privacy Association

November 22, 2005

Philippa Lawson
Executive Director and General Counsel, CIPPIC

The conflict between privacy and security, while perhaps evident to those of you who deal with access to information requests on a daily basis, has only become a burning public issue in the post-9/11 world, as individuals are detained on the basis of secret evidence, as police seek greater surveillance powers, and as we experiment with increasingly invasive methods of identifying terrorist threats.

But is the issue really one of necessary trade-offs between privacy and security? I'd like to take a closer look at what we mean by security, and whether the measures that we are taking to enhance our security in fact likely to do so.

First, a few words about privacy - privacy is not just a question of confidentiality – rather, it is about the right to control information about oneself.

As the Supreme Court of Canada has pointed out, our “notion of privacy derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit”.

Privacy is also not just a question of personal boundaries – rather, a fundamental aspect of civil liberties, affecting society as a whole as well as individuals.

That's why we have enshrined in the *Charter of Rights and Freedoms*, the "right to be secure against unreasonable search and seizure", as well as the "right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice."

These safeguards against state incursions constitute a critical “line in the sand” when it comes to state security measures – our guidelines for ensuring a balance between privacy and traditional notions of security.

Many recent examples of the clash between privacy and security indicate an all-too-ready willingness on the part of Canadian governments and law enforcement agencies to sacrifice very concrete privacy interests for a extremely nebulous notion of security.

I'll start with **Access to Information**, since that's the focus of so much of your work.

Access to information, including access to one's personal information held by government, is an important component of civil liberties; I don't need to explain to you why this is the case

You know more than I do about the challenges and practices in this area, so I won't dwell on it. Just a few words about the exercise of discretion to refuse access on the grounds of national security:

In a recent decision, an adjudicator for the Ontario IPC found that the Ottawa police's attempt to invoke a blanket "national security" exemption to withhold all information requested by the Ottawa Citizen about their handling of the G20 and G8 meetings in 2001 and 2003 was overblown. While he agreed that some of the information was properly withheld, he found the broad-brush denial of all records on the basis of vague and general reasons to be unacceptable. Refusals to disclose should be specific and specifically justified.

The requirement for specific justification of refusals to provide access, and for severance and provision of information that need not be withheld, is an important safeguard against abuse. Information that does not need to be withheld, should not be withheld. This requires more effort on the part of people like you, but surely that effort is worth the payoff in terms of government accountability and, in the case of access to personal information, privacy.

Turning to the more obvious issue of Canada's response to 9/11 and the global terrorism threat:

While Canada's incursions of civil liberties may not have been as extreme as some other countries, we are, I believe, guilty of a knee-jerk reaction to perceived security threats that provides us with very little actual security but does so at very great cost to certain individuals and to our society at large.

The *Anti-Terrorism Act*, for example, provides for new state powers to detain terror suspects under "**security certificates**". These certificates allow the detention and arrest of non-citizens on the basis of secret evidence (no opportunity to defend oneself). Moreover, the standard of proof is "reasonableness"- far lower than the normal criminal law standard of "beyond a reasonable doubt". Not surprisingly, the security certificate provisions are being appealed to the Supreme Court of Canada.

Five individuals are currently being held under these provisions in Canada – they have no way of defending themselves against phantom charges. For them, it is a Kafkaesque nightmare. Are the rest of us any safer as a result?

We all know the story of **Maher Arar**. One man's life ruined by over-zealous security agencies sharing information about a suspect and acting on that information without allowing the suspect any opportunity to respond to the allegations or to defend himself – in other words, violating fundamental safeguards of justice that protect our privacy and liberty.

And although it should be commended for finally agreeing to hold a public inquiry on the matter, the gov't continues to withhold key information, depriving Arar of the ability to properly defend himself and clear his name. How much safer are we as a result of the sharing of information that led to Maher Arar's ordeal?

The **Public Safety Act** provides more examples of inappropriate trading-off of privacy in the name of security. Among other things, the Act revises PIPEDA, so as to permit private sector organizations to surreptitiously collect and use personal information for national security purposes. Previously, companies were permitted to disclose such information to state authorities, but this amendment takes a significant step in the direction of totalitarian state power, by putting private corps in position of acting as agents of state, and allowing them to spy on their customers. Were citizens of Maoist China, Iraq or the former East Germany more secure as a result of the widespread private spying that went on in those states?

And finally, the latest salvo in the federal government's attempt to beef up security: Bill C-74, or the **Modernization of Investigative Techniques Act**. This is part of a broader package of legislative initiatives called "Lawful Access", but perhaps better referred to as "Facilitating Surveillance", or as some have suggested, "Reducing Privacy".

Lawful Access is about expanding police investigatory powers and facilitating surveillance in digital environment. The police say that they are stymied by new technologies and need more powers to continue to do their job rooting out crime, now that criminals can communicate anonymously over the Internet.

Now, to its credit, Canada is not proposing to construct a national database of subscriber information, nor is it proposing mandatory retention of subscriber data by telecom service providers, nor is it proposing *USA PATRIOT Act*-style powers that permit law enforcement agencies to access detailed customer records from service providers upon request.

But the government is proposing, under *MITA*, to improve surveillance capacity in Canada in two respects:

1. A requirement for all telecom service providers to be technically capable of permitting police interceptions. Right now, the police say they are sometimes technically obstructed from conducting interceptions simply because of the way an ISP is configured. This new law would force ISPs to ensure that new and upgraded facilities are intercept capable. It would thus, over time, ensure the creation of a communications architecture that

facilitates surveillance – not only by the police, but by the communications providers themselves.

Technology has been whittling away at our privacy for years. But here’s a case where the technology in a way *protects* us. The government wants to strip away such *de facto* protections, so that we are left only with legal safeguards.

But the second part of the bill involves *removing* a legal safeguard: the ability of TSPs to require a warrant before handing over subscriber information to the police. Bill C-74 would give the police (and CSIS) warrantless access to name, address, telephone number, email address, and/or IP address of subscribers, upon provision of one such piece of identifying data. It includes a number of safeguards, such as the requirement that such requests be documented, justified in terms of their relevance to the law enforcement agency’s duties or functions, and subject to regular internal audits and discretionary external audits.

But it lacks a fundamental privacy protection: the requirement for independent third party authorization, under a standard of “reasonable and probable grounds”, before police can engage in searches or surveillance.

The government says that name, address, and other identifying information does not attract a reasonable expectation of privacy sufficient to invoke the warrant requirement. That question may eventually be put to the courts. Certainly, many internet users would disagree.

Name and address are keys to all sorts of sensitive personal information (much of it available by simple Internet searches) - financial information in public records, information about websites one visits on the Internet and communications with others online. Many people use pseudonyms on the Internet in order to engage in anonymous communications without fear of embarrassment or retribution. They have a high expectation of privacy in relation to their Internet identities, and reasonably so. Unmasking their identities without any kind of judicial authorization or even requirement for reasonable cause to suspect criminal behaviour is, I would argue, in the nature of a search and should therefore be subject to the same protections against abuse.

Moreover, internal auditing does not replace auditing by an independent external party. Surely, we have learned enough lessons from our own history to know that state surveillance powers will be abused if not kept in check. How much safer are we if police can link our name with our online activities , without any real grounds for suspicion?

In all of these cases, we are giving up fundamental privacy protections in order to protect ourselves against evil-doers. But in each case, it is unclear that we have accomplished anything in terms of greater security.

We need to ask the same questions of new security measures such as biometric passports, national ID cards, and no-fly lists, that have been proposed or are on track to be introduced in Canada. In each case, there are serious privacy trade-offs. And in each case, we are told that the security benefits outweigh the privacy costs. But is that really the case?

How exactly will **biometric passports** make us safer? Aside from all the operational problems associated with biometrics, border guards don't screen for terrorists on the basis of fingerprints - as security expert Bruce Schnier points out, there is no fingerprint database for suspected terrorists!

Creating a biometric database of everyone who travels will do a good job of providing governments with the ability to monitor and control their citizens, but it won't protect us from terrorists. If the goal is a global surveillance society, then biometric passports make a lot of sense. But if the goal is real security – from all threats including states – then it fails the test.

Again following the lead of the US, Canada is preparing to introduce a **Passenger Screening** system – first, a “no fly” list of people considered too risky to allow on flights, but not necessarily suspect enough to be charged with a criminal offence. The longer term plan is an automated system of screening passengers “to provide an enhanced level of security”.

This initiative comes despite clear evidence from the US that no-fly lists result in all sorts of false positives, without any guarantee of filtering out suicide bombers. Profiling is rife with problems, aside from its privacy implications for individuals and society at large. There are always bad guys who don't fit the profile (no history; no previous links to terrorism), and there are always innocent people who fit the bad guy profile.

Profiling actually gives smart criminals an easy way of avoiding detection: they just need to make efforts to establish a normal-looking profile. Passenger screening is unlikely to be an effective security measure, but is likely to instill fear in all of us – fear of the authorities, not the criminals.

And many experts have pointed out that **National ID cards** will make us less secure – by, among other things, requiring the existence of a central database on everyone. Huge databases such as this are guaranteed to have failures, failures that are exploitable by criminals.

All of these measures add up to significant incursions on individual privacy in order to achieve greater security. It seems that privacy and security are on an inevitable collision course, and that, wherever they collide, we have to make difficult choices about which should take precedence.

But the erosion of privacy does not necessarily lead to greater security - terrorists will always find ways to get around state security measures, and will always be a step ahead of law enforcement. Deft criminals can take advantage of some so-called security measures to hide their identities or otherwise evade capture.

The more data about us that is collected, stored, traded, and otherwise out of our control, the more likely it is that fraudsters and terrorists will find ways to access and take advantage of that data. We are already seeing the security fallout from the growing trade in personal information, in the form of identity-theft related crimes.

The answer to this problem is not to develop ever-more sophisticated ways of tracking and identifying people, it is instead in limiting the collection and trade in personal information in both public and private sectors.

We do need more effective authentication mechanisms – especially if we want to make the most of the Internet and online access to information – but such mechanisms need not trade privacy for security. They can and should be designed to minimize the collection and use of personal information. Indeed, the strongest authentication mechanisms are those that do not require any sacrifice of privacy. Every time we collect, store, or disclose personal information in order to enhance security, we are not only reducing individual privacy and facilitating the disruption – or worse, devastation – of individual lives by over-zealous authorities, but we are also risking the access and abuse of such information by unauthorized third parties.

In conclusion, I'd like to pick up on another point made by Bruce Schneier – that security, like privacy, is a multi-faceted notion. That is, it's about not just our security against terrorism and criminals, it's also about our security against tyrannical governments. Unchecked police and government powers are just as much of a threat to our security as is unchecked terrorism.

Limits on government power and guarantees of due process are security measures. Principles of fair and open justice are security measures.

So it doesn't make sense to sacrifice fundamental rights and freedoms in the name of security. We should never be decreasing oversight and accountability while increasing law enforcement powers. In fact, as the opportunities for electronic surveillance grow and as the cost of surveillance drops, we need to be enhancing oversight and accountability mechanisms.

Rather than opposites, security and privacy are inextricably linked. Real security can't be achieved without effective privacy protections.

*** END ***