Reflections on Public Interests and Private Rights: Conflict or Convergence?

William PENTNEY*

Introduction

Let me begin with a story. Let's say you have a daughter, a teenage daughter, who has just started to date the high school football star. You know the type — basking in the glow of hero worship and vaguely smelling of cheap cologne, eating more than a small horse, and apparently running purely on hormones. Or perhaps you have a teenage son who has just started to date the high school beauty queen — you know the type, full of eye shadow and self-confidence, she learned long ago the power she has over boys, just by a flick of her hair or a glance across a room, and you fear she has broken more hearts than you care to count. You are not thinking kind thoughts — whether it is your son or your daughter, you are thinking that this way lies trouble, and you want to help before someone you love deeply gets hurt. If only you knew what was going on when you're not around.

Rest easy, help is on the way. There is a cell phone that anyone can purchase over the Internet in Europe that may be just the ticket. This is a very special little device. It looks just like any other phone, and it works just fine for your son or daughter. There is one feature that you may have forgotten to mention, however — this phone comes with a special phone number. When you dial it the phone does not turn on, it does not ring, it does not buzz or play a song. Instead, it turns into a monitoring device, allowing you to listen to any conversation going on

* Senior Assistant Deputy Minister, Policy Sector, Department of Justice, Ottawa, Ontario. The views expressed in this paper are my own, and do not represent the positions of the Department of Justice nor the Government of Canada. The author would like to thank Joseph Langan for his able assistance in the preparation of this paper for publication.

within earshot of the phone. And before any parents rush out to make the purchase, let me add that I am advised that this little gadget is illegal in Canada.

This may seem like an odd way to start a talk about information technology and national security, in the context of a conference about "Technology, Privacy and Justice." I start here perhaps because I am the father of two university-aged young women, and sometimes I think less-than-charitable thoughts about certain young men. More seriously, this story is a good place to start because it nicely illustrates the theme of my talk, which is about how technology has now evolved to the point where there is a growing convergence between public interests and private rights.

I want to suggest that the usual analysis that national security measures are taking away our privacy, and that it is technology that facilitates that loss, is a perfectly valid way of looking at the matter, but there may be other equally illuminating perspectives. The traditional analysis pits privacy rights against national security interests, and assumes that more of one must mean less of the other. It focuses on the power of the state to gather, analyze and share information about people, and asks whether there are sufficient controls in place to properly regulate this activity. These are important and legitimate questions, and they must be widely and thoroughly debated.[1]

I want to go at this in a slightly different way, by suggesting that there are actually three important ways in which public interests and private rights converge in this area: first, in the technologies themselves, and their capacities for good and evil; second, in the interests that these technologies affect; and finally, in relation to the concerns that we have (or ought to have) about the legal and moral frameworks that are applied to them. Before exploring the theme of convergence, I need to set out a definition of the term "national security" so that we are all working with a shared understanding of the concept.

---

[1] See *The Security of Freedom: Essays on Canada's Anti-terrorism Bill*, edited by R.J. Daniels, P. Macklem and K. Roach (Toronto, Ontario: University of Toronto Press, 2001) and S.H. Cohen, *Privacy, Crime and Terror: Legal Rights and Security in a Time of Peril* (Markham, Ontario: LexisNexis Canada, 2005)

National Security in Canada

In April 2004 the federal government issued the first-ever National Security Policy for Canada, under the title "Securing an Open Society."[2] The federal policy begins with the statement: "There can be no greater role, no more important obligation for a government, than the protection and safety of its citizens."[3] It then identifies three core national security interests:

1. protecting Canada and Canadians at home and abroad;

2. ensuring Canada is not a base for threats to our allies; and

3. contributing to international security.[4]

This framework is rooted in Canadian values and Canadian laws, beginning with the *Charter of Rights and Freedoms*, which embodies our deep and abiding commitment to a free and democratic society, dedicated to ensuring freedom, equality and the right to "life, liberty and the security of the person."[5]

From this, the Policy sets out a definition of national security which embraces more than just terrorism; issued in the shadow of the SARS crisis, the Policy rightly takes a wider view:

> National security deals with threats that have the potential to undermine the security of the state or society. These threats generally require a national response, as they are

---

2 See http://www.pco-bcp.gc.ca/docs/Publications/NatSecurnat/natsecurnat_e.pdf

3 *Ibid.*

4 *Ibid.*

5 *Constitution Act, 1982,* being Schedule B of the *Canada Act 1982* (U.K.), 1982, c. 11. See also the Preamble to Bill C-36, *An Act to amend the Criminal Code, the Official Secrets Act, the Proceeds of Crime (Money Laundering)Act and other Acts, and to enact measures respecting the registration of charities, in order to combat terrorism*, assented to 18th of December, 2001 First Session, Thirty-seventh Parliament, 49-50 Elizabeth II, 2001

> beyond the capacity of individuals, communities or provinces to address alone.[6]

The Policy then goes on to list a number of current threats to the national security of Canada, including terrorism, the proliferation of weapons of mass destruction, foreign espionage, natural disasters, organized crime, and "critical infrastructure vulnerability." On this last threat, the Policy states that cyber-attacks "are a growing concern that have the potential to impact on a wide range of critical infrastructure that is connected through computer networks."[7]

The Policy recognizes that cyber-security is a pressing issue which involves both the public and private sectors, and that improving our capacity to prevent cyber-attacks, and to control and contain the effects of those that occur, must involve close cooperation between the public and the private sector.[8]

This is a good place to begin to explore the main theme of my remarks, which is about convergence.

I. Shared Technologies

The old hands in the national security world tell me that back in the "good old days", the government had a monopoly on all of the neat technology. That was when "spooks were spooks", and the rest of us could only wonder where they got their toys.

Today, of course, technology has changed all that. I described the cell phone monitor earlier. Combine that with advances in video and audio surveillance, remote sensing and computer programs that allow you to hack into a keyboard secretly to record every stroke. It is child's play to record a conversation from 100 yards. New technology allows you to pick up the heat signature of a person lying in a bed from across the street, and to monitor his conversation through a closed window by extracting the longitudinal vibrations transmitted through two panes of glass. This is

---

6 *Supra* note 2

7 *Supra* note 2.

8 *Ibid.*

all available, as they say "COTS", which stands for "commercial, off-the-shelf."[9]

Now don't get me wrong, governments have the best of the best, and it is truly amazing what can be done. But the public's increased access to these types of technologies and others has fundamentally changed the rules, for both private citizens and for governments. Protection of critical infrastructure involves not just protecting government secrets and computer systems from foreign spies; we now need to guard against the same hackers who gum up your home computer with useless spam, and occasionally with evil viruses.

Private sector capacities to gather data, to congregate it in truly staggering databases, and to manipulate or analyze it for their own purposes now comes closer than ever before to matching or exceeding any systems that governments can develop. A story in the Guardian newspaper from England describes how a major supermarket chain, set up a subsidiary to develop a database, called "Crucible", that is "collating detailed information on every household in the UK, whether they choose to shop at the retailer or not".[10] This database includes socio-economic and lifestyle characteristics, drawn from public and private databases, and is sold to a variety of companies. This database does not merely gather information, it permits manipulation of the raw data for the purposes of analysis and conjecture about future shopping habits.[11]

Now this is a reasonably minor example, and no doubt you have heard about the United States government's efforts after the 9-11 terrorist attacks to create a super-database called "Total Information Awareness".[12] My point is simply that governments create these databases under the glare of unremitting scrutiny, which is as it should be, but we must wonder

---

9 See W. Atkinson, "They're watching you", *Globe and Mail*, (10 September 2005) F7 for a description of modern, commercially-available, surveillance technology.

10 H. Tomlinson, R. Evans, "Tesco stocks up on inside knowledge of shoppers' lives", (20 September 2005) (www.guardian.co.uk/business/story/0,3604,1573821,00.html).

11 *Ibid.*

12 See American Bar Association, National Security Law Report Vol. 27, No. 1 (Feb. 2005), for a discussion of this and other initiatives. This is a special issue on the Cantigny Conference on "Counterterroism Technology and Privacy".

about the powers that the new technologies give to those outside of government with the resources and motivation to harness them.

There is another dimension to this convergence. The private sector's access to new technologies poses ever-greater threats to the security of government information and systems, not to mention expanding the capacity for private industrial espionage on competitors at home and abroad. The digital revolution has changed the assumptions for public and private security, because it has taken away the usual markers of time, route and space [the markers need to be explained- people outside the field may not recognize them]. In the hard-wired world we grew up in, police needed only to get access to the number where a call originated, or the phone which received it. If that was not possible, they could tap into the wire over which it passed, and trace it up and down the line to find out who was on either end.

In today's digital wireless world, you may be able to pick up bits of digital information as it zooms along the system, but this won't get you much. First, the sender and receiver may be identified (if at all) by a numeric internet address, which cannot be linked to any physical location. Even if you know where they are supposed to be, wireless access defeat that assumption. And since digital information is transmitted in electronic packets which are easily encrypted or are simply split up and sent over different routes before being re-assembled at one end point (as is common in Voice Over Internet communications), you may have no way of "reading" the full message anyway. In this sense, the new technologies make it more difficult for the state, or for private industry, to keep up with the capabilities of those who seek to do harm.

The digital world does have elements which enhance the capacity of the state and private sector to keep their information secure [is there a tension between private citizens keeping information secure and governments and businesses doing so?]. Modern digital communications systems generate "traffic data", which can be stored and analyzed to determine what went where, when and how. And computer databases now offer the capacity to maintain records of who went looking where, and when. Digital systems operate in such a way that any interception along the way will leave a "digital footprint" that simply cannot be avoided or eliminated, if the system is designed properly. These two elements provide the capability to design systems which can be audited randomly and can support both quality control and individualized investigations.

This offers to government and private corporations the assurance that they can trace and investigate security breaches. It also offers to individuals (and the oversight and review agencies that protect their interests) the capability to find out who has had access to their private information, and for what purpose. In this sense, there is a shared interest in designing intelligent systems which meet legitimate needs while respecting privacy to the fullest extent technologically possible,[13] and in maintaining traffic data for a reasonable period of time.[14]

At the same time, of course, the new technologies also offer ever-greater capacities to protect, to monitor and respond to threats of hacking or outright attack on computer systems, and to respond to national or private emergencies by linking people and harnessing information as never before. So the effects are not all negative; in truth, almost all of the technology is inherently benign. We know that most of the people who use cell phones, baby monitors, and the Internet do so for perfectly innocent reasons. We also know that both public and private infrastructure has been attacked by people who do so for the thrill of surreptitiously going where they are not allowed, and sometimes who seek to destroy on a wide scale.

A key point here is that those in the private and public sectors who think about how to protect security must deal with the reality that most uses and most users of technologies do so for perfectly legitimate purposes, but at the same time, hidden among the thousands of innocents, are methodical criminals and terrorists who are using the Internet and these surveillance and data technologies for evil means. The Director of CSIS, in testimony before a House of Commons Committee earlier this year, stated:

> [T]he terrorist networks responsible for or associated with the 9-11 attacks have become more physically dispersed and simultaneously much more technologically sophisticated in how they operate and how they

---

13 On this point, see J. Rosen, *The Naked Crowd : Reclaiming Security and Freedom in an Anxious Age* (Random House, 2004).

14 See *Data Retention Directive*, 21 September 2005 Memo/05/328, online: European Union (www.europa.eu.int/rapid/pressReleasesAction.).

> communicate. The terrorist networks' use of the Internet for example as a communications, recruitment, and propoganda tool has been truly impressive in bolstering their capacity around the world and again in our own country through the use of sophisticated encryption, the techniques of stenography, the use of the Internet as a purveyor of videos for the recruitment of new adherents and the use of multiple e-mail accounts by many suspects.[15]

Much of this cannot be discussed publicly, for reasons you will understand. A recent story in the Washington Post gives a rare glimpse into this world. The story begins like this:

> In the snow-draped mountains near Jalalabad in November 2001, as the Taliban collapsed and al Qaeda lost its Afghan sanctuary, Osama bin Laden biographer Hamid Mir watched "every second al Qaeda member carrying a laptop computer along with a Kalasknikov" as they prepared to scatter into hiding and exile.[16]

It carries on to describe how the Internet has become a haven for communication, fund-raising and operational planning for terrorists, as al Qaeda morphs from a highly structured organization into a loose coalition of like-minded individuals spread across continents.[17] The most fascinating example of this is the description of how terrorists have adapted and innovated to exploit the possibilities of the Web, while seeking to avoid detection:

---

15 Speaking Notes of the Chief of CSE before the Special Senate Committee undertaking a Parliamentary Review of the *Anti-Terrorism* Act, April 11, 2005. Avaialble online : (http://www.cse-cst.gc.ca/documents/about-cse/ccse-anti-terrorist-act-11april2005-e.pdf)

16 S. Coll and S. Glasser, "Terrorists Turn to the Web as Base of Operations", *Washington Post*, (7 August 2005) A1. See also G. Weimann, "www.terror.net : How Modern Terrorism Uses the Internet" (March 2004), United States Institute of Peace, Special Report online: (www.usip.org).

17 *Ibid.*

> Kahlid Sheik Mohammed, a key planner of the Sept. 11 attacks later arrested in Pakistan, used what researchers familiar with the technique called an electronic or virtual "dead drop" on the Web to avoid having his e-mails intercepted by eavesdroppers in the United States or allied governments. Mohammed or his operatives would open an account on a free, public e-mail service such as Hotmail, write a message in draft form, save it as a draft, then transmit the e-mail account name and password during chatter on a relatively secure message board… The intended recipient could then open the e-mail account and read the draft — since no e-mail was sent, there was a reduced risk of interception…[18]

So my first point is that there is a convergence of risks and advantages that flows from these technologies, for both the private sector (including big multinationals and you and me when we use our home computers or cell phones[19]), and the public sector — whether it is in the business of gathering "intelligence" or simply trying to keep secure the personal records of citizens or employees.

And from the perspective of the individual, there is convergence as well, because we now must think about the technological power possessed by both the private and public sectors, and be wary of both. Which leads me to my second theme.

II. Shared Interests

In the face of this convergence of risks and rewards associated with new technologies in this world of national security, there is also a convergence of fundamental interests: security, privacy, equality of treatment, and governance according to the rule of law.

---

18 *Ibid.*

19 See J Gatehouse, "You are Exposed: When Even the Privacy Commissioner's Cellphone Records Are Available Online, We've All Got Security Problems" *MacLean's,* (21 November 2005).

I have dealt with the shared public and private interest in security in the last section. The shared interest in privacy may seem counter-intuitive to those who fear the power of the state, so let me begin to explore that aspect. We need to begin with the simple fact that public entities every bit as much as private citizens, value privacy defined here at its most basic — the right (or the opportunity?), to be left alone. Both public institutions and private individuals have things they want to guard secret, sometimes for legitimate reasons and sometimes just to avoid embarrassment. We have enacted elaborate laws governing when public institutions can enjoy that luxury, and this is certainly the subject of much controversy and debate in Ottawa and elsewhere these days.[20] But the simple fact remains that it is not only private citizens who value privacy — at the level of high principle this interest converges for public institutions, private corporations, and private citizens.

This is not to say, however, that these interests are the same, nor are the capacities to interfere with privacy equally distributed. There is no doubt that the state stands in a special position vis-à-vis both companies and citizens, since it alone has a monopoly on such coercive powers as search, arrest, detention and imprisonment. So I do not claim that the privacy interests are the same; I am content to make the more modest claim that there is a convergence of interests in being left alone, and a shared interest in keeping safe that which is truly secret.[21]

This is a special challenge in the face of the emerging technologies, and we have augmented our laws to permit the agencies of the federal state who protect our critical information infrastructure — the Department of Public Safety and Emergency Preparedness, and the Communications Security Establishment — to undertake this task.[22]

---

20 See the *Privacy Act* (R.S., 1985, c. P-21) and the *Access to Information Act* (R.S., 1985, c. A-1).

21 See, for example, cases where the government is seeking to protect privacy interests in the face of Access to Information requests: *Canada (Information Commissioner)* v. *Canada (Commissioner of the RCMP),* (2003) 1 S.C.R. 66; 2003 SCC 8; *H.J. Heniz Co. of Canada Ltd.* v. *Canada (A.G.)* 2006 SCC 13.

22 For a description of the roles of each, see their public websites; http://www.cse-cst.gc.ca and http://www.psepc.gc.ca/. Also see in particular the testimony of the Chief of C.S.E. before the Special Senate Committee reviewing the Anti-Terrorism Act, April 11, 2005 on line : (http://www.cse-cst.gc.ca/documents/about-cse/ccse-

There remains a question, however, as to whether the current laws and policies are adequate to protect individuals' privacy rights — do we have the right framework to deal with the digital age, and the age of terror? There is no easy answer to this. Unlike the private sector, governments operate under the *Charter of Rights and Freedoms*, which offers substantial protection of privacy rights as defined by the Supreme Court.[23] In addition, there are statutes (the *Privacy Act*[24] and the *Personal Information Protection and Electronic Documents Act - "P.I.P.E.D.A."*[25]) which govern the collection and use of personal information by the state and private sector. One question which has emerged is whether these instruments, which fundamentally look at each situation one-by-one, are adequate to enable us to have a cumulative view — the citizens' view. Another question is whether there needs to be stronger internal checks and balances. The Department of Justice plays a significant role in determining whether proposed laws and regulations will withstand Charter scrutiny, and this is an important counter-balance to those within government who may wish to pursue policies which Justice's legal analysis concludes would go beyond what the Charter will allow.[26] There remains the question of whether this, together with the privacy officials who operate in each Department, and the Privacy Commissioner, provide sufficient capacity to understand and to mitigate the cumulative privacy impacts on individuals in Canada. This is not a question which is easily answered, but it must be debated.[27]

The second shared interest is in ensuring equality of treatment, which in turn is closely linked with the concept of governance according to the rule of law. By a shared interest in equality of treatment, I mean two things: first, there is a shared interest in ensuring that there is no *a*

---

anti-terrorist-act-11april2005-e.pdf.) *supra* note 15. This offers a rare glimpse into the work and priorities of the C.S.E.

23 *Supra* note 5.

24 R.S., 1985, c. P-21.

25 2000, c.5.

26 See M. Rosenberg and W.F. Pentney, "That We Can Become Better than We Are: Imagining Canadians and the *Charter* in 20 Years" (2003) 19 Sup. Ct. L. Rev. (2d) 439.

27 See the Privacy Commissioner's 2004-2005 Annual Report to Parliament on the *Privacy Act* available at (http://www.privcom.gc.ca/information/ar/200405/200405_pa_e.asp)

priori difference in treatment either with respect to access to or use of the new technologies. Neither the public nor the private sectors have an interest in establishing or maintaining some kind of "digital divide" within the populace at large. Both have invested heavily in making the infrastructure necessary to support the Internet, for example, as widely available to all sectors of society as possible. I am not claiming that equal access has been achieved; anyone living in a remote community would tell you otherwise, but these are not due to active efforts to exclude.[28]

The second shared interest in equality of treatment relates to the rules which govern any restrictions that are placed on access to or use of the Internet. For the private sector and governments alike, there is a shared interest in living under a set of rules which provide for standards of fair treatment rather than the anarchy of private self-help.

This plays out differently for the private and public sectors, of course, but those who have studied the Internet know that there is a very active population of knowledgeable activists who have dealt with private efforts to enforce rules or practices which are perceived to be unfair, through a form of cyber-justice which is both subtle and effective. Anyone who has read stories of companies that receive constant streams of faxes of blacked-out pages sent over the Internet (using up toner in the fax machine at an alarming rate), or thousands upon thousands of repeat messages to tie up servers and slow down business, will realize that there is an active self-help movement which guards the inner morality of the Net.

Public authorities, of course, are held to constitutional and statutory standards, and those with the most extreme intrusive powers are also subjected to intensive review and oversight.[29]

---

28 See the Report of the National Broadband Task Force, available at (http://broadband.gc.ca/pub/program/NBTF/broadband.pdf)

29 For example, see the Annual Reports of the Security Intelligence Review Committee, on line at (http://www.sirc-csars.gc.ca/reports_e.html), which deal with CSIS, and the Reports of the Commissioner of the C.S.E., former Chief Justice Antonio Lamer, available on line at (http://csec-ccst.gc.ca/index_e.php). The issue of review of the national security activities of the R.C.M.P. is currently being reviewed by Justice O'Connor in the Arar Inquiry, under Part II of his mandate (available on line at http://www.ararcommission.ca/eng/12.htm.)

In the area of national security, these interests converge because public and private entities, and individuals, share common goals, even if they do not operate within the same legal frameworks.

III. Shared Concerns

My last point of convergence is that there are (or, I suggest, there ought to be) shared concerns on the part of ordinary citizens, about both the public and private sectors, in relation to national security. I will not try to deal comprehensively with these concerns; instead, I will ask and attempt to sketch out answers to some of the questions which seem to me to be important here, hopefully as a basis for stimulating discussion.

I begin with a simple question: how much security do we want? How much security from terrorism, whether manifested as cyber-attacks or bombs on subways? After 9-11 it seemed that Canadians wanted a great deal of security, and they wanted it quick. As time passes, we need to continue to talk about this, to come to a clearer understanding of just how much security can realistically be provided, and at what cost to our society (whether measured in dollars, values, habits or assumptions).

Similarly, we need to ask how much security we expect private companies to provide? We have all seen news reports about thefts of computers which contain confidential customer or government data, or of private banking information mistakenly faxed to a wrecking yard somewhere. This provokes a storm of media coverage, and the obligatory apologies and investigations by the corporation, but it should also lead us to think about how much security we want private companies to provide, and what we should do to achieve that. In the area of national security, there is one further convergence here — because we increasingly need private companies to conduct their own security measures to protect infrastructure, to guard both commercial and governmental secrets, and to prevent their high-tech systems from being used as the platform for terrorist attacks.

This discussion leads to a consideration of the type of legal framework which is appropriate in relation to these types of technology. The recent initiative known as “lawful access” is intended to modernize the laws to keep pace with the evolving technologies, and to adapt the

words to the digital age — but the underlying legal frameworks are meant to remain in place.[30] The state should still generally require a search warrant, or its digital equivalent, before accessing your private communications. We need to debate what the appropriate framework is in relation to other types of information (for example, what standard should be applied to the traffic data which simply shows the route a message followed, or the basic customer information which is the equivalent of what I can find in any telephone book?) These need to be debated, as do a host of more technical questions.

But at this stage, no one is suggesting that the basic underlying framework, the core balance between state power and individual privacy, should be set aside. What is needed is a continual debate about how this shared framework can be adapted and applied in a sensible way to information technology systems which are no longer rooted in time or space, and which verge on becoming exercises of the imagination — as we chase digital bytes of information over the Internet, the concepts of "search warrants" and "telephone intercepts" seem less and less relevant to the exercise, even if the underlying concepts still apply. We may need a new language to describe the reality of a digital world.

A final question that I want to leave you with relates to the legal framework at an even higher level. We have treated almost all aspects of information technology as a private good, to be developed, bought, sold and exploited as private industry sees fit. Yet in other areas such as biotechnology, there are intense debates about the basic moral framework for understanding what the technology now permits us to do. We sometimes talk about uses of this genetic technology as being unacceptable on moral grounds. Efforts are underway in Canada and elsewhere to develop legal frameworks that will set the boundaries around this technology, to reflect our shared moral consciousness.

Would the same analysis ever apply to information technology? Are there some applications, some new gadgets that we would say are simply morally unacceptable? We have come to accept "nanny cams",

---

30 See the *Lawful Access Consultation Paper* (Department of Justice, Solicitor General Canada, Industry Canada), Augusat 25, 2002, (available online at http://www.justice.gc.ca/en/cons/la_al/consultation_index.html). See also: *The Modernization of Investigative Techniques Act*, Bill C-74, tabled in the 38th Parliament, November 15, 2005. This Bill died on the Order Paper when the last federal election was called.

even while we express discomfort with closed-circuit TVs in public places. We accept surreptitious video surveillance by private investigators, and ubiquitous camera phones, yet at the same time we rail against traffic light cameras in plain view. The taxi I came to this hotel in had a very visible camera trained on me, and my driver said it made him feel safe — but I as a customer had no meaningful opportunity to choose whether to be filmed or not, because all of the cabs are now similarly equipped.

The question I have is whether we as a society will reach a point where we want to consider whether to place limits on the development or use of these technologies, or whether we are content to leave it to the private market to set the boundaries of what is acceptable. This is a big question, and I do not pretend to have an answer. It is, however, time for a public debate about the issue; both the power and the awesome promise of this technology demands it.