The State of Privacy in the Canadian State: Fallout from 9/11

Colin Bennett* and Martin French**

Introduction

The literature on privacy and surveillance is rich and varied. Scholars, journalists, practitioners, and others from many nations have analysed the causes and consequences of the excessive collection and processing of personal information, and debated the merits of a range of legal, self-regulatory and technological solutions (Bennett and Grant, 1999). With few exceptions, most of this literature would share the following four assumptions: 1) privacy is an individual right; 2) privacy is something that we once had but is now eroding; 3) the privacy problem arises from structural and organisational forces that together reduce the ability of individuals to control the circulation of their information; and, 4) the organisations that are responsible for privacy invasion can be observed, resisted and regulated because they are subject to the laws of discrete and bounded liberal democratic states. These assumptions constitute the 'privacy paradigm' (Bennett and Raab, 2003).

In contemporary circumstances, each of these assumptions can be questioned. Privacy protection can be regarded as a social value as much as it is an individual one (Regan, 1995). To argue that privacy is vanishing, eroding, dying and so on (e.g. Whitaker, 1999; Rosen, 2000), assumes that antecedent agricultural and industrial societies offered higher ''levels'' of privacy than conditions in current post-industrial societies, an assumption which is highly problematic. The sources of privacy invasions are also complex. The picture of an embattled individual trying to stem the tide of surveillance flowing from a range of impersonal and invulnerable structural forces makes good rhetoric for the privacy cause, but it distorts reality and oversimplifies social and political analysis. Privacy problems arise from a complex interplay of structure and agency. They occur when technologies work and when they fail, when humans have worthy motives and when they do not.

However, the subject matter of this article most closely relates to the last assumption. The privacy paradigm tends to be state-centric in two different senses. First, the right to privacy is generally regarded as a benefit of state citizenship. This right is conferred on us by virtue of our national identities, be they Dutch, American, British, Canadian, or any other. The privacy and data protection laws, which provide us with certain guarantees about our personal information, reflect some essential principles of liberal democracy that are either enshrined in constitutions (such as in the US Fourth Amendment) or deeply embedded in the cultural and historical experiences of different societies.

Second, contemporary discourse and policy prescriptions are generally dictated by a paradigm which suggests that our personal information still tends to be held within organisations that are easily identifiable and that operate within the boundaries of modern territorial states. It is not simply that the forces of globalisation have necessitated harmonised international solutions to the privacy problem; the growing policy interdependence has caused a proliferation in the number of transnational actors, and a progressive frequency and regularity of networking opportunities. It might be assumed that this transnational policy-making has caused a concomitant reduction in state sovereignty. The question is not, any more, whether data protection policy should be made at the international or the national governmental levels; data protection policy is, and must be, made at both levels. Rather, the question is how national and international regimes interact to respond to an inherently transnational policy problem caused by a global economy. Privacy is a global problem, and it is being addressed through a repertoire of policy instruments that also know few attachments to traditional conceptions of legal and territorial sovereignties (Bennett and Raab, 2003).

This article charts the Canadian policy responses to the acts of terrorism on 11 September 2001. In brief, we argue that before 11 September, Canadian privacy protection policy had diverged in some significant ways with that of the United States. Policy developments were very much driven by international pressures, but from

Department of Political Science, University of Victoria, Victoria, B.C., V8W 3P5, Canada *E-mail: cjb@uvic.ca
**E-mail: martian@uvic.ca

Europe, rather than from the United States. We discuss three sets of responses by the Canadian government to 11 September, in the areas of law enforcement, international travel, and Internet surveillance. Within these policy fields, the narrowing rights of suspects, the collecting and processing of passenger information, and the monitoring of Internet ''traffic data'', all indicate the diminished importance of privacy post-9/11. On these issues, Canadian policy has been forced to converge with that of the United States, thus undermining prior attempts to distinguish Canada as a more privacy-friendly society than the US, in which citizens enjoyed a more complete set of rights to informational self-determination.

An Overview of Canadian and American Privacy Protection Policy

Historically, approaches to the issue of privacy protection have differed substantially between the United States and Canada. Through statutory and constitutional measures, the control over the collection, processing and disclosure of personal information tends to be a lot stronger in Canada than in the United States. A more complete set of data protection laws exists for the regulation of personal data processing in Canadian public agencies, than in their American counterparts. These laws are overseen by a network of privacy and information commissioners that operate at both federal and provincial levels (Bennett and Bayley, 1999). Table 1 provides a current overview of the status of public sector privacy legislation in Canada.

It is with respect to data protection controls in the private sector, however, that the cross-national differences are most notable. On 1 January 2001 the Protection of Personal Information and Electronic Documents Act (PIPEDA) came into force in Canada. With this legislation, the Canadian government brought Canada more closely into line with most other countries (except the US and Japan) within the advanced industrial world PIPEDA comes into force in stages. On 1 January 2001 the following business sectors were obliged to comply: banking, telecommunications, broadcasting, airlines, and transportation companies, as well as any company that sells personal information across provincial or national borders, including many involved in e-commerce. After 3 years, the law will apply to all commercial activities undertaken

Table 1: Status of public sector privacy legislation in Canada

Jurisdiction	Name of act	Date proclaimed	Oversight agency
Federal	Privacy Act	1982	Privacy Commissioner of Canada
Alberta	Freedom of Information and Protection of Privacy Act	1995	Office of the Information and Privacy Commissioner
British Columbia	Freedom of Information and Protection of Privacy Act	1993	Office of the Information and Privacy Commissioner
Manitoba	Freedom of Information and Protection of Privacy Act	1997	Office of the Manitoba Ombudsman
New Brunswick	Protection of Personal Information Act	2000	Office of the Ombudsman
Newfoundland	Privacy Act	1996	Director of Legal Services, Department of Justice
Nova Scotia	Freedom of Information and Protection of Privacy Act	1994	FOI and Protection of Privacy Review Officer
Ontario	Freedom of Information and Protection of Privacy Act	1988	Information and Privacy Commissioner/Ontario
Prince Edward Island	Freedom of Information and Protection of Privacy Act	2001	Assistant Clerk of the Committee Legislative Assembly
Quebec	An act respecting access to documents held by public bodies and the protection of personal information	1982	La Commission d'accès à l'information du Quebec
Saskatchewan	Freedom of Information and Protection of Privacy Act	1992	Information, Privacy and Conflict of Interest Commissioner
North West Territories/ Nunavut	Access to Information and Protection of Privacy Act	1996	Information and Privacy Commissioner
Yukon Territory	Access to Information and Protection of Privacy Act	1996	Office of the Ombudsman

Table 2: Status of General Privacy Protection Law for the Private Sector

Jurisdiction	Act or other official action	Date
Federal	Protection of Personal Information and Electronic Documents Act	2001
Alberta	Internal review of issue	
British Columbia	Legislative Committee Report	2001
	Government Discussion Paper	2002
Manitoba	Discussion Document Published	1999
New Brunswick	Discussion Document Published	1998
Newfoundland	No known official action	
Nova Scotia	No known official action	
Ontario	Discussion document published. Bill in preparation	2001
Prince Edward Island	No known action	
Quebec	Bill C-68 (An Act respecting the Protection of Personal Information in the Private Sector)	1993
Saskatchewan	No known action	
North West Territories/Nunavut	No known action	
Yukon	No known action	

by the private sector, including companies under provincial or territorial jurisdiction, unless the provinces pass ''substantially similar'' legislation in the meantime. If they do not, PIPEDA will apply by default to the retail sector, the manufacturing sector, most insurance companies, video-rental outlets, and indeed to most businesses that have face-to-face relations with consumers. Thus the provincial governments are now deciding whether they want to pass their own statutes, or to do nothing and surrender an important constitutional power to the federal government; a decision that would possibly have implications for federal/provincial relations beyond that of privacy (Perrin et al. 2001; Berzins, 2002). Table 2 presents the current status of initiatives with regard to private sector privacy protection.

In the United States, the protection of personal information within private corporations is reliant on the implementation of a more complicated patchwork of federal and state laws that only apply to quite specific categories of personal information: consumer credit information, video-rental records, insurance records, and so on. More recently, Congress has moved to provide protections for personal privacy within the financial sector (the Gramm-Bleach-Bliley Act) and to protect children's privacy (the Children's Online Privacy Protection Act). A highly controversial set of regulations to protect health information has also been issued by the Department of Health and Human Services. Some businesses have moved to self-regulate in order to protect privacy, motivated in part by the need to continue to receive personal information for processing from European suppliers and clients; the ''Safe-Harbour'' agreement encourages businesses involved in international personal data transmissions to commit themselves to some basic privacy principles. Breaching these principles would constitute an 'unfair and deceptive' trade practice and would contravene Federal Trade Commission (FTC) rules. In total, however, privacy protection in the private sector is still fragmented and incomplete (Gellman, 1993).

Crude economic analysis would perhaps have predicted that Canada would not wish to diverge in any significant way from American privacy protection policy for fear that businesses might relocate south of the border to take advantage of the less restrictive regulatory climate. This brief sketch serves to demonstrate that Canada chose to take a very different path from its major trading-partner to the south. There are some significant domestic reasons why Canada chose a more interventionist policy than did the United States.

Explaining the Divergence

Typically, differences between Canadian and American public policy are explained in terms of cultural factors. Canadians are supposed to be more accepting of state intervention and more suspicious of the unregulated marketplace. This supposed cultural difference does not help to explain why different data protection policies are being pursued.

Some comparative poll results suggest that Canadian and US attitudes about privacy and

how to protect it are strikingly similar. Seventy-eight percent of Americans believe that 'consumers have lost all control over how personal information about them is circulated and used by companies'; seventy percent of Canadians believe the same. In response to the question: 'Which type of invasions of privacy worry you most today – activities of government agencies or businesses?' fifty-two percent of Americans, and fifty-one percent of Canadians say government; forty percent of Americans and thirty-seven percent of Canadians say businesses. In 1994, fifty-one percent of Americans reported that they felt 'very concerned' about threats to personal privacy; thirty-seven percent of Canadians felt that way. The differences in policy response can be explained neither by greater fears for privacy among the Canadian public than the American, nor by greater trust of business in the U.S. than in Canada (Harris and Westin, 1994:17).

The differences in policy also cannot be explained in terms of the differential extra-territorial impact of the European Union's Data Protection Directive, which stipulates that personal data on Europeans should not flow from the EU to countries that cannot guarantee an 'adequate level of protection' (EU, 1995). There is certainly some fear that larger American multinationals can afford to take care of their interests within the European policy arena more effectively than their smaller counterparts and subsidiaries in Canada. But Canada does relatively little trade with the EU. The United States is significantly more important to the Canadian economy, than is the EU. Proportionately, the EU is relatively more important to the US economy than it is to the Canadian. The enforcement of Articles 25 and 26 of the EU Directive is far more likely to disrupt the trade in goods and services from Europe to the United States, than from Europe to Canada.

The difference is also not explained by the presence of a stronger and more vocal ''privacy lobby'' in Canada. If anything, the privacy advocates in the United States have been more influential (especially on issues relating to online privacy protection) than have the disparate band of consumer advocates, civil libertarians, academic experts and private consultants in Canada, who share few common perspectives and interests. The policy process in Canada has not been attended by public debate, or by an enormous clamouring for reform by outside interests. This is fairly typical of the policy process for data protection in other countries. There has been a constant, but low-key, stream of media attention, but nothing that would captivate the attention of federal politicians and force them to act.

We would argue that the main differences are explained more by domestic political and economic factors. Canadian data protection policy is a patchwork (as in the United States). But the impact of this incoherence on Canadian business has been more serious than has the lack of coherence in the U.S. been for American business.

The first difference relates to the early enactment of a private sector privacy protection law in the province of Quebec. For businesses that operate in different provinces and jurisdictions, the transaction costs of having to deal with different privacy laws and regulations can create uncertainty and confusion. Hence, this is a particularly acute problem for provincially regulated industries, such as insurance and retail. Such enterprises are obliged to grant rights to Quebec consumers that citizens in other parts of the country do not enjoy. Some businesses have thus harmonised their rules and declared that their practices in the rest of Canada conform to the Quebec standard. It is for these reasons that the rhetoric about ''marketplace rules-of-the road'' and ''level-playing fields'' on the information highway tended to overshadow the traditional discourse about human rights and civil liberties. It is also the reason why the lead department was Industry Canada, rather than Justice Canada (Bennett, 1996).

A second factor relates to the network of trade associations in Canada, which tend to be more inclusive than their counterparts in the United States. The impact of ''free-riders'' in some industrial sectors is therefore more keenly felt. The Canadian Marketing Association (CMA), for example, claims that its members are responsible for around eighty percent of the direct-marketing activity within Canada. These companies are expected to abide by the CMA's privacy code (if they wish to remain members). The reputation and indeed economic interests of the majority are then harmed by the actions of the minority (which may collect and trade in personal data without regard for consent rules or the mail and telephone preference services). The CMA became the first association in Canada to call for national legislation to protect privacy in October 1995.

The final factor is the existence of a small network of privacy and information commissioners, not present in the United States. Most provinces now have such officials, who on occasion can speak forcefully and concertedly for stronger privacy protections. Commissioners have been especially worried that the protection offered by legislation like the federal Privacy Act is circumvented when ''private'' organisations perform ''public'' functions, and require the use of ''public'' data to fulfil those obligations. Together, these factors pushed Canada in the direction of the vast majority of advanced industrial states that have sought comprehensive and statutory solutions to the problem, and away from the policy of its largest trading partner,

which continues to rely on an incremental, fragmented and self-regulatory approach.

Canadian Privacy Protection Policy after 11 September

The events of 11 September had the immediate effect of shifting the focal point of privacy protection policy from the traditional problem of domestic harmonisation for economic reasons, to the new problem of international harmonisation for security reasons. Most notably, initiatives to create a ''common security zone'' within North America have significant implications for Canadian privacy protection policy. Even though none of the perpetrators of the 11 September attacks entered the United States via the Canadian border, there is nevertheless a perception that Canada provides a safe-haven from which terrorist activity against the United States can be planned. For example, U.S. officials have criticised Canadian immigration and refugee laws as too lax, citing the case of Ahmed Ressam, a failed refugee applicant from Algeria, who was arrested in December 1999 while trying to cross the border into Washington State with explosives in the trunk of his car. Ressam was later convicted on charges of plotting to bomb Los Angeles International Airport during millennium celebrations. In the name of creating a ''common security zone'' around Canada and the US, a number of Canadian laws and policies are currently under review. With specific regard to privacy protection, however, several legislative initiatives are worthy of analysis.

To begin this analysis, it would be useful to draw a distinction, however murky, between two kinds of privacy: *fundamental privacy* and *strategic privacy*. This analytical distinction illuminates the disjuncture in the privacy protection discourse between privacy as an essential value, and privacy as a value to be balanced with other values. In general, and on a sociological level, the concept of privacy is often used in some fundamental sense. Hence, where privacy denotes certain *fundamental* values, its protection is generally posed as an *a priori* good. When, for example, the Canadian Privacy Commissioner, George Radwanski, refers to privacy as 'a fundamental human right' or as 'an innate human need', he is using the term privacy in this fundamental sense (Radwanski, 2002a).

At the level of public policy, the concept of privacy is rarely framed in a fundamental sense. Rather, the pragmatic mindset of policy makers tends to produce a *strategic* understanding of privacy. Where privacy denotes certain *strategic* values, privacy interests are specifically balanced against other interests. Hence, the need for institutional privacy protection might be seen as flowing from the eclipse of privacy interests by other, more powerful, organisational interests. One role of the Office of the Privacy Commissioner, therefore, is to mitigate the compromises made in policy between privacy and other interests, and sometimes the Commissioner has been able to justify his critiques of policy through an ultimate appeal to the fundamental nature of privacy. However, following 11 September, the importance of the fundamental meaning of privacy, like other fundamental rights, was immediately diminished. In terms of privacy protection, the after-effect of 11 September was to make the strategic meaning of privacy instrumentally more dominant in the discourse.

Three sets of responses by the Canadian government to 11 September reflect the withdrawal of fundamental privacy from the post-9/11 privacy protection agenda. Although 2001 began with the implementation of strong privacy protection legislation (PIPEDA), it ended with widespread emergency amendments that pose a significant threat to the privacy rights of Canadians. The most troubling effect of 9/11, however, has been the normalisation, in 2002, of an emergency mentality in numerous policy areas. The domination of a *strategic* approach to privacy and the concomitant normalisation of the emergency mentality are nowhere more evident than in the policy fields of law enforcement, international travel, and Internet surveillance.

Law Enforcement – Powers of Arrest and Detention

By far the most comprehensive response to 11 September was the Anti-Terrorism Act, (hereafter Bill C-36), an omnibus and varied set of measures designed to enhance the federal government's ability to prevent and detect terrorist activity. Bill C-36 modifies more than twenty pieces of legislation, including the Federal Privacy Act and PIPEDA. In its preamble, the Bill states that:

> 'the challenge of eradicating terrorism, with its sophisticated and trans-border nature, requires enhanced international co-operation and a strengthening of Canada's capacity to suppress, investigate and incapacitate terrorist activity' (Canada, 2001a)

Bill C-36 creates a brand new category of criminal offence based on new definitions of ''terrorist activity'', ''terrorist group'', as well as ''facilitation'' and ''participation'' in terrorist activity. The draft legislation initially had a very broad definition of terrorism. This definition was narrowed by the time Bill C-36 was passed. However, the definition remains sufficiently

broad to give cause for concern. Where the state can demonstrate that a threat of terrorism exists - not a difficult task considering the breadth of the ''terrorist activity'' definition - extensive and powerful surveillance and enforcement tools can be brought to bear on suspects. For instance, section 83.18(2)(c) of the act makes indictable the participation in a terrorist group, regardless of whether or not 'the accused knows the specific nature of any terrorist activity that may be facilitated or carried out by a terrorist group' (Canada, 2001a). This section suggests that, depending on the state's discretion in the naming of a terrorist group, one could come under the broad powers of surveillance enumerated in Bill C-36 by virtue of their association with a suspect organisation.

Most controversially, the bill provides police forces and government with new and considerable powers, often of a discretionary nature. Bill C-36 introduces fundamental changes to commonly held rules of justice, notably in matters such as arrest, detention and wiretapping. The bill also permits preventive detention up to 24 hours without any charge for a criminal offence. The legislation also makes the authorisation of communications surveillance much easier to obtain (Canada, 2001a). The considerable powers thus provided to law enforcement and security agencies permit them to interrogate, monitor, detain and open files on any individual without any other basis than mere suspicion of participation in a 'terrorist activity', as it is defined in the bill. Arguably, the legislation raises enormous potential for racial discrimination. Since 11 September, anti-racist organisations have vocally criticised Bill C-36 for targeting visible minorities.

Each of these provisions raises important privacy questions. Many of the reforms involve record keeping and disclosure obligations that have a direct impact on privacy (Austin, 2001). The Federal Privacy Commissioner, however, decided that these wider battles over Canadian civil liberties could not be successfully fought. The bill, he concluded, was a ''well-balanced, well thought-out effort to enhance security to give law enforcement authorities the measures they need to be able to effectively seek to combat terrorism, while at the same time respecting privacy rights that are maximum possible'' (Radwanski, 2001a). He therefore decided to focus his attention on a provision that was clearly within his remit – the rights of individuals to obtain information about themselves under both the Privacy Act and PIPEDA.

Following the first reading of Bill C-36, the Privacy Commissioner pointed out that certain proposed amendments to the Privacy Act not only removed limitations on the state's use of citizen information, it also removed the scrutiny of his oversight. The Commissioner argued:

> 'The way the law is written, the minister could issue a certificate that says, disclosure of information by CSIS, the Canadian Security Establishment or a department of government, or indeed all departments of government, could be taken off the table. At that point, not only would there be no possible disclosure and no oversight of that, but according to this, all the other provisions of the Privacy Act would not apply. So there would be no limitations on how the information could be used, combined, shared or disclosed. In effect, these provisions could be used to nullify the Privacy Act by ministerial fiat.' (Radwanski, 2001a)

After several weeks of private negotiation and public wrangling, the Minister of Justice introduced a number of amendments to C-36 that effectively met the Commissioner's concerns.

In response, Mr. Radwanski wrote an open letter to the Minister praising her action 'as a great victory for the privacy rights of all Canadians. You have reaffirmed on behalf of the Government of Canada that privacy is a fundamental human right that, even in times of gravest crisis, must always benefit from the maximum protection possible' (Radwanski, 2001b). This effusive praise prompted one of the opposition leaders to accuse Radwanski of 'climbing down' under pressure, an accusation that prompted another open letter from the Privacy Commissioner (Radwanski, 2001c).

There is no doubt that the narrowing of these provisions constituted a certain victory for the Privacy Commissioner's position. However, in the wider context of the legislation, the questions concerning access to personal information under the Privacy Act and PIPEDA, do seem relatively narrow. Consequently, we conclude that, in the law enforcement policy field, fundamental privacy has been trimmed out of policy discourse in two ways. First, in the immediate climate of emergency following 11 September, the Privacy Commissioner was only able to effectively address the infringement of information privacy and not privacy more generally. Second, where the Commissioner scrutinised legislation, he also was compelled to discuss privacy in a strategic way. In this regard, the policy discourse focused on privacy as an interest to be balanced with security. While the Commissioner had never claimed that privacy was an absolute right, neither had he ever so frequently juxtaposed his concerns with security issues.

International Travel

On 22 November, not quite two months after the 11 September attacks, the government

introduced the Public Safety Act, initially known as Bill C-42, which, among other things, amended the Aeronautics Act with regard to the disclosure of passenger travel data to law enforcement agencies. A week later, the government introduced An Act to Amend the Aeronautics Act (hereafter Bill C-44), which was created by removing a small section from Bill C-42. This law facilitates the sharing of passenger lists on flights coming into, and leaving, Canada.

Bill C-44 was hived off for quick passage when it became clear that the broader Bill C-42 – the second and accompanying legislation to C-36 – would not pass in time to meet a 18 January deadline set by the United States; President George W. Bush signed a law in November, 2001 requiring foreign airlines to provide passenger lists and other basic information to U.S. authorities. Bill C-44 stipulates:

> 'an operator of an aircraft departing from Canada or of a Canadian aircraft departing from any place outside Canada may, in accordance with the regulations, provide to a competent authority in a foreign state any information that is in its control relating to persons on board or expected to be on board the aircraft and that is required by the laws of the foreign state' (Canada, 2001b)

This provision overrides Section 5 of the Personal Information Protection and Electronic Documents Act.

Reflecting on the domestic impact of the Canadian-American legislative amalgamation in this field, Radwanski remarked:

> 'Authorising aircraft operators to disregard the Personal Information Protection and Electronic Documents Act and provide the authorities of foreign countries with ''any'' personal information about Canadian travellers required by the laws of such countries is an extremely serious matter. It is particularly troubling when the laws of those countries, as in the case of the U.S., provide no safeguards or restrictions as to how such information may subsequently be used or to what third parties, including other countries, it may be disclosed. It is possible to envisage circumstances in which this could put Canadians at very real risk' (Radwanski, 2001d)

He was also concerned that the government of Canada 'should not end up with a backdoor access to information that it might not otherwise have to Canadians'. He therefore recommended an amendment that would restrict these agreements to share information collected for the purposes of protecting national security, and restricting its further use or disclosure for any other purpose (Radwanski, 2001d). In response, the government tabled an amendment that would prohibit the Canadian government from obtaining information supplied by Canadian airlines to foreign authorities. This has the somewhat peculiar result that the US and other governments could obtain such information, but the Canadian Government itself could not. Nevertheless, Radwanski accepted the amendment, whilst still articulating concerns over the unnecessary scope of the bill.

While Bill C-44 remains intact, Bill C-42, which had a number of problems, was withdrawn in April 2002. The new Public Safety Act, now known as Bill C-55, has been substantially corrected. However, one section of C-55 remains a source of concern for the Privacy Commissioner. Section 4.82 of the Act would:

> 'give the RCMP and CSIS unrestricted access to the personal information of all Canadian air travelers, on flights within Canada as well as on international routes […] In Canada, police forces cannot normally compel businesses to provide personal information about citizens unless they obtain a warrant. Section 4.82 would entitle the national police force and the national security service to demand personal information about all Canadian air travelers without any judicial authorisation.' (Radwanski, 2002b)

This section has sparked a considerable and heated public debate between the Privacy Commissioner, the Solicitor General, and the Minister of Transport. In an exchange with the Solicitor General, the Privacy Commissioner began to distance himself from the practice of justifying all extreme legislative measures with reference to the terrorist attacks of 11 September (Radwanski, 2002c).

And yet, in spite of the Commissioner's recent exhortations, the government continues to produce progressively more invasive policy. The Canada Customs and Revenue Agency (hereafter CCRA) is currently taking steps to compile Advance Passenger Information and Passenger Name Records in an integrated database. The Advance Passenger Information system contains a traveller's name, date of birth, gender, travel document information, and nationality. The Passenger Name Record system is considerably more detailed. It lists a traveller's destination, method of ticket purchase, seat selection, number of pieces of checked luggage, and the date the ticket was booked. The CCRA intends to keep this information for unspecified customs purposes. The Privacy Commissioner has noted that the database could be used for virtually any purpose the government deems appropriate. These could include: data matches with other departments, income tax audits, as well as criminal investigation 'fishing expeditions' (Radwanski, 2002d).

Internet Surveillance

The effects of 11 September seem to be reverberating as deeply through the *cyber* world as they are through the *real* world. As part of the anti-terrorism package, the Canadian Government also signed the Council of Europe's Convention on Cyber-Crime. The Convention was broadly accepted by around 30 advanced industrial states as necessary following the 11 September strike (CoE, 2001). This agreement has a number of implications for the way personal information is treated. For instance, the Convention could require organisations to provide the government with their encryption keys, raising issues of privacy and self-incrimination. Other provisions require laws that allow the state to collect and record the data traffic of service providers. These provisions would regularise law enforcement's use of software like the Carnivore diagnostic tool. The Convention also stipulates that data be retained for criminal investigation. The data warehousing that would stem from this stipulation raises concerns about the creation of huge amounts of searchable information about people. With the implementation of the Convention, there is concern about the balance shifting further away from privacy in favour of security (Austin, 2001).

The Department of Justice, Industry Canada, and the Solicitor General co-released a consultation document on ''lawful access'' on 25 August 2002. In the context of Internet surveillance, or more broadly telecommunications surveillance, lawful access allows law enforcement agencies to intercept communications. The consultation document opens by noting that surveillance tools have been instrumental in securing convictions for criminal activity. On the agenda are several amendments to different pieces of legislation. These amendments would update Canada's wiretap laws, giving enforcement agencies the capacity to lawfully snoop on wireless technology.

Most of the amendments up for debate would require service providers (SPs) to supply infrastructure that would ensure the state's capability to intercept information. There is currently no such mechanism in Canadian law. At the outset, it is unclear as to what organisations will qualify as SPs. The working definition states that a SP is 'a person who owns or operates a transmission facility that is used by that person or another person to provide telecommunications services to the public in Canada' (Canada, 2002). Given that there are so many different kinds of service providers with different levels of infrastructure (including universities), the lawful access policy will likely have quite differential effects. In terms of data protection standards, it is difficult to understand how principles will be equally applied. Particularly interesting is the discussion on data-preservation orders. Here, data preservation is distinguished from data retention. Data preservation involves serving a judicial order to preserve specific information whereas data retention is a general requirement to retain a range of data concerning all subscribers. Neither practice is likely to be appealing to privacy advocates, who perceive this distinction as spurious.

These, then, are the principal policy initiatives introduced to date that have a direct bearing on the collection, processing and disclosure of personal information under Canadian law. As in the United States, a range of technological measures are also being seriously contemplated, including enhanced video-surveillance at airports with facial recognition capability, retinal and/or hand geometry scanning, more sophisticated profiling of airline passengers, more complex programs of data matching, and so on. There has also been a debate about identity cards. The federal government has announced that immigrants to Canada will get a new plastic photo ID card instead of articles that are easily forged. The Minister said that the new immigration card, called the Maple Leaf, will have fraud-proof technology including laser imprinting and a magnetic strip to store encoded ''tombstone data''.

Conclusions

This summary of some of the policy developments since 11 September permits a number of tentative conclusions about the ''state of privacy'' in Canada. And the picture is very ambivalent. Polls still demonstrate that Canadians are very concerned about how their privacy is being eroded by a range of social and technological threats. On the other hand, a recent Gallup poll indicated that seventy-two percent of Canadians think it is more important for police to intercept communication between suspected terrorists than it is for the government to protect the privacy of the public (Ottawa Citizen, 2001). The cases outlined above permit, nevertheless, three broad conclusions about the post-9/11 state of privacy in Canada.

Firstly, until 11 September, the Canadian federal political system had been making some important strides towards a more comprehensive set of safeguards for personal data protection. Public opinion polls were largely supportive of wider privacy laws, for both public and private sectors, and some clear differences were emerging between Canadian and US policy. To a large extent these trends are still continuing. The provinces are seriously engaged in attempting to pass ''substantially similar'' privacy protection laws in their jurisdictions. The implementation of PIPEDA has begun, albeit slowly and haltingly, and the Privacy Commissioner is releasing a

number of quite strong investigative reports on private sector practices. It is tempting to conclude, therefore, that privacy protection policy has become limited to those more mundane aspects of privacy protection. The development of techniques for protecting privacy in the everyday world of credit-card purchases and direct-marketing practices may appear to be a diversion for privacy advocates and regulators to busy themselves with while the ''real business'' of heightening surveillance for internal security proceeds apace (Bennett and Raab, 2003). But these private sector realms cannot be insulated from the world of security and surveillance. The shaping of specific business processes is also being affected by the pressure of these other policy considerations.

Secondly, and with regard to law enforcement issues, privacy protection has been defined more and more narrowly within the Canadian State. To the extent that it involves the collection, processing and disclosure of personal information, the issue can be advanced by the Privacy Commissioner of Canada. However, this formulation elides deeper surveillance issues. The greater issues concerning enhanced surveillance powers for law enforcement when a broadly defined crime of ''terrorism'' is suspected were never seriously addressed by the Privacy Commissioner. These legislative and policy actions indicate that the Privacy Commissioner's ability to prevent state infringement on privacy rights is diminishing. Where the public sector has determined to use personal information to combat the threat of terrorism, the advocacy of the Privacy Commissioner has seemingly little impact. As the emergency mentality has become normalised and instruments of the state have been more consistently directed towards security, privacy, conceived in a strategic sense, is trumped. A weak and fragmented coalition of civil liberties and public interest groups protested, but also had little effect on either the content or the timing of these measures.

Finally, although the historical record has yet to be thoroughly researched, it is probable that significant pressures to converge with dominant American practices are the main explanation for all of the various policy changes. At a time, therefore, when Canadian privacy protection policy was beginning to diverge from, and be more progressive than, that in the US, 11 September has convinced many American policy makers that American security is only as strong as that of the longest undefended border in the world. And those arguments have obviously had a powerful influence on the Canadian federal government.

But this is not a story of indigenously created Canadian privacy protection policy being challenged and undermined by US influence. Canadian privacy law has been likewise shaped by the force of international agreements (especially those struck in Europe). The governance of privacy in the global economy takes place through multiple modes of regulation and co-ordination. Simply because privacy standards are being traded-up and enforced in some arenas, does not mean that surveillance practices are being correspondingly reduced. There are sufficient institutional arenas for the issue to advance sufficiently well in some, and at the same time to regress elsewhere. This article has shown that in Canada, at least at the moment, those advances are seen in relation to private sector, rather than public sector practices. But it is thoroughly misleading to try to observe a single ''balance'' between privacy and surveillance on a global, or even a national, scale (Bennett and Raab, 2003).

References

Austin, L. (2001), 'Is Privacy a Casualty of the War on Terrorism?' in Daniels, R., Macklem, P. and Roach, K. (Eds), *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill*, University of Toronto Press, Toronto, pp. 251–267.

Bennett, C. (1996), 'Rules of the Road and Level Playing-Fields: The Politics of Data Protection in Canada's Private Sector,' *International Review of Administrative Sciences*, volume 62, pp. 479–491.

Bennett, C. and Bayley, R. (1999), 'The New Public Administration of Information: Canadian Approaches to Access and Privacy,' in Wesmacott, M. and Mellon, H. (Eds), *Public Administration and Policy: Governing in Challenging Times*, Prentice Hall Allyn and Bacon, Scarborough.

Bennett, C. and Grant, R. (Eds), (1999), *Visions of Privacy: Policy Choices for the Digital Age*, University of Toronto Press, Toronto.

Bennett, C. and Raab, C. (2003), *The Governance of Privacy: Policy Instruments in Global Perspective*, Ashgate, Aldershot.

Berzins, C. (2002), 'Protecting Personal Information in Canada's Private Sector: The Price of Consensus Building,' *Queens Law Journal*, volume 27, pp. 609–645.

Canada (2001a), *Anti-Terrorism Act - An Act to Amend the Criminal Code, the Official Secrets Act, the Canada Evidence 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*, Department of Justice, Minister of Supply and Services, Ottawa, on-line at: http://www.parl.gc.ca/37/1/parlbus/chambus/house/bills/government/C-36/C-36_4/C-36TOCE.html.

Canada (2001b), *An Act to Amend the Aeronautics Act*, Department of Justice, Minister of Supply and Services, Ottawa, on-line at: http://www.parl.gc.ca/37/1/parlbus/chambus/house/bills/government/C-44/C-44_4/90175bE.html.

Canada (2002), '*Lawful Access – Consultation Document*', Department of Justice, Industry Canada, and the Solicitor General of Canada, Minister of Supply and Services, Ottawa, on-line at: http://canada.justice.gc.ca/en/cons/la_al/a.html#2.

Council of Europe (CoE) (2001), *Legal Co-operation*: *Cyercrime*, Council of Europe, Strasbourg, on-line at: http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Combating_economic_crime/Cybercrime/.

European Union (EU) (1995), *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Brussels, OJ No. L281, (The EU Data Protection Directive) (24 October 1995).

Gellman, R.M. (1993), 'Fragmented, Incomplete and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions,' *Software Law Journal*, volume 6, pp. 199–231.

Harris, L. and Westin, A. (1994), *The Equifax-Canada report on Consumers and Privacy in the Information Age*, Equifax Canada, Ville d'Anjou.

Ottawa Citizen (2001), 'Security trumps privacy: poll 72% willing to sacrifice privacy to help police catch terrorists', 22 November 2001, Ottawa.

Perrin, S., Black, H., Flaherty, D. and Rankin, T. (2001), *The Personal Information Protection and Electronic Documents Act: An Annotated Guide*, Irwin Law Inc., Toronto.

Regan, P. (1995), *Legislating Privacy: Technology, Social Values and Public Policy*, University of North Carolina Press, Chapel Hill.

Radwanski, G. (2001a), *Testimony Before the House of Commons* Standing Committee on Justice and Human Rights, 23 October 2001, on-line at: http://www.privcom.gc.ca/speech/02_05_a_011024_e.asp.

Radwanski, G. (2001b), *Letter from the Privacy Commissioner of Canada to the Minister of Justice*, 21 November 2001, on-line at: http://www.privcom.gc.ca/media/nr-c/02_05_b_011121_e.asp.

Radwanski, G. (2001c), *Letter from the Privacy Commissioner of Canada to the Rt. Hon. Joe Clark, leader of the PC/DR Coalition*, 22 November 2001, on-line at: http://www.privcom.gc.ca/media/nr-c/02_05_b_011122_e.asp.

Radwanski, G. (2001d), *Letter from the Privacy Commissioner, George Radwanski to the Minister of Transport*, 30 November 2001, on-line at: http://www.privcom.gc.ca/media/nr-c/02_05_b_011130_e.asp.

Radwanski, G. (2002a), *Legal Education Conference – Privacy*: *Your Rights and Obligations* Speech delivered at the Community Legal Information Association of PEI', 17 October 2002, on-line at: http://www.privcom.gc.ca/speech/02_05_a_021017_e.asp.

Radwanski, G. (2002b), *Statement by the Privacy Commissioner of Canada on Bill C-55*, 1 May 2002, on-line at:http://www.privcom.gc.ca/media/nr-c/02_05_b_020501_e.asp.

Radwanski, G. (2002c), *Letter from the Privacy Commissioner of Canada to the Solicitor General of Canada on the subject of Bill C-55*, 17 May 2002, on-line at: http://www.privcom.gc.ca/media/nr-c/02_05_b_020517_e.asp.

Radwanski, G. (2002d), *Letter to the Hon. Elinor, Caplan, Minister of National Revenue*, 26 September 2002, on-line at: http://www.privcom.gc.ca/media/nr-c/02_05_b_020926_3_e.asp.

Rosen, J. (2000), *The UnWanted Gaze: The Destruction of Privacy in America*, Vintage Books, New York.

Whitaker, R. (1999), *The End of Privacy: How Total Surveillance is Becoming a Reality*, New Press, New York.