Counterpoint

Archives and Privacy in a Wired World: The Impact of the *Personal Information Act* (Bill C-6) on Archives*

TIM COOK

RÉSUMÉ Dans cette période informatique de l'Internet et du courrier électronique, des bases de données transnationales et du commerce électronique, on peut constater une peur grandissante que les renseignements personnels soient vendus aux plus offrants et que la confidentialité soit constamment érodée. Le gouvernement canadien a entendu et répondu à ses citoyens ainsi qu'à la communauté internationale qui demandait des normes plus serrées. La *Loi sur les renseignements personnels* de 2000 (projet de loi C-6) met en place les conditions auxquelles les compagnies privées et les individus doivent se conformer pour protéger les informations personnelles. Cependant, les défenseurs de la confidentialité ont fait valoir que des mesures plus fortes encore étaient nécessaires.

Cet article examine l'impact de la *Loi sur les renseignements personnels* sur les centres d'archives. En effet, afin de protéger la confidentialité et les renseignements personnels, la législation et les défenseurs de la confidentialité semblent prêts à sacrifier divers aspects de la culture et de l'histoire. Les archivistes doivent s'assurer que cela ne se produira pas et trouver un équilibre entre les atteintes à la confidentialité et le besoin des Canadiens de se connaître, de même que leur passé et leur histoire collective.

ABSTRACT In this electronic age of Internet and e-mail, transnational databases, and electronic-commerce, there is a growing fear that personal information is sold to the highest bidder and privacy is steadily being eroded. The Canadian government has listened and responded, both to its citizens and the international community that has demanded tighter rules. The *Personal Information Act* of 2000 (Bill C-6) sets out the conditions by which private companies and individuals must conform to safeguard personal information. But privacy advocates have argued that stronger measures are needed.

This article examines the impact of the *Personal Information Act* on archives. In the interest of protecting privacy and personal information, privacy legislation and advocates seem willing to sacrifice aspects of our culture and history. Archivists must ensure that this is not the case and find a balance between privacy infringement and the need for all Canadians to know themselves, their heritage, and their collective history.

* The ideas in this paper are those of the author and do not necessarily reflect the position of the National Archives of Canada. The author would like to thank Terry Cook, Brian Beaven, Cathy Bailey, and Cara Downey for their valuable comments.

At the dawn of the Millennium, there is a growing apprehension that our collective privacy, one of the most important tenets of democracy, is being steadily eroded in the face of new technology. In this electronic age of the Internet and e-mail, transnational databases, and electronic-commerce, individuals are continually giving personal information to governments and private companies. It is almost impossible to avoid this wired world and its related documentation, even though few feel comfortable with this new electronic frontier where, as in the Wild West, there seems to be only a few regulators imperfectly enforcing new laws.

In the name of efficiency, data matching is becoming a regular tool of businesses and governments. Certainly, the linking of two databases by itself does not constitute a loss of privacy. According to some observers, the problem is how that matched data is used for secondary purposes. Each reported case of a fifteen-year-old hacker breaking into the databases of the most powerful companies in the world from his basement computer, each example of a government agency inadvertently releasing personal information, each instance of privacy infringement by companies – both domestic and international – with their growing range of information on individuals, leaves citizens feeling more uneasy. Not surprisingly, then, there has been a push by citizens and their champions to stop the slide towards arbitrary and unauthorized disclosure of personal information in digital format.

The Canadian government has listened and responded, both to its citizens and the international community that has demanded tighter rules, by recently introducing new legislation to complement the existing *Privacy Act* of 1983. Bill C-6, *the Personal Information Protection and Electronic Documents Act*, was tabled in the House of Commons in 1998 (as Bill C-54) and eventually assented to law (as Bill C-6) in 2000. The *Personal Information Act* will be described in more detail below, but very briefly, it sets out the conditions to which private companies and individuals must conform in safeguarding personal information. The Act goes a long way to redress the legislative gap relating to personal information in the private sector. But the battle for control of privacy has not stopped there. Privacy advocates have argued that stronger measures are needed. As one group of commentators remarked at an academic roundtable discussion on the issue: "privacy is and always has been under attack in the western world."[1] Others have even suggested that personal information must be controlled by the individual who created it or to whom it relates – even if they wish to see it destroyed. And it is here, at the nexus of privacy and non-disclosure versus access to records and freedom of inquiry, that privacy advocates and archivists have been, and will continue to be, in

1 As brought up in the round table discussion, "Human Rights and Information Technology Issues," *Proceedings from Privacy & Information Technology: Friend or Foe?* (New Brunswick: privately published, 1997), p. 7.

conflict. In the interest of protecting our collective culture and history, archivists must not only be aware of these issues, but quite possibly pit themselves against privacy advocates in this struggle over contested ground and concepts.

Some privacy advocates have suggested that once data has been compiled and used for its original purpose, it should be destroyed, arguing that any type of information can be used against citizens. This includes data as valuable to historians, local and family researchers, and legal scholars as the national census itself. Some advocates go further, asserting that the right to protect sensitive personal information does not die with the individual, but is a perpetual right transcending death and inherited by subsequent generations. Some also believe that all personal information is sensitive, rather than particular categories for particular time periods. By this mind-set, government accountability, individual rights, history, and heritage are to be sacrificed to this fear over possible misuse of personal information. Such an action is damaging, shortsighted, and not in the interest of citizens. The destruction of archival records to accommodate privacy concerns will imperil the rights of all Canadians to know one another, to understand themselves, and to embrace their place within Canadian society and history.

Privacy Infringement

In order to comprehend the competing views of privacy groups and archivists, it is necessary to understand first the concerns of those advocating new and, in the eyes of many in the archival profession, heritage-damaging action. Privacy is difficult to define but one commentator has noted that it refers to the "condition of being protected from unwanted access by others – either by physical access, personal information or attention."[2] For most Canadians, privacy is an essential concern. Reflecting the importance of the issue, privacy watchdog groups, consisting of federal and provincial commissioners, organized advocacy groups, and concerned citizens, are a powerful lobby in our society. They are driven by the belief that our collective privacy is steadily being eroded by governments, large corporations, and even fellow citizens. In much of the discourse surrounding the topic, there remain important symbols of oppression.

The spectre of George Orwell's novel, *1984*, has cast a shadow over much of the later half of the twentieth century. It continues to spark concerns over loss of personal freedom that now extend to debates over privacy and the Internet. As one of the most important novels ever written, *1984* was crafted after the Second World War and at the onset of the Cold War. Its chilling tale of repression, totalitarism, collectivity, and thought-control became a poignant warning of unfettered state power. In history, the frenzied butchering of their

2 Sissela Bok, *Secrets: On the Ethics of Concealment and Revelation* (Vintage Books, 1984) pp. 10–11.

external enemies and their own citizens by the totalitarian states eventually led to their own destruction. Yet it has been the slower, more insidious process of terror, the surveillance of all citizens, the indoctrination of the young, and the control of history that has proved more difficult to overcome. One of the most disturbing aspects of *1984* is that we never know how the Big Brother-haunted society degenerated, except that it occurred after a war. And that, of course, has encouraged privacy advocates to point fingers at a variety of problems in modern society, warning and lamenting that unless we respond now, we could, in the near future, be living in an Orwellian dystopia.

Along with the disturbing surveillance prevalent throughout *1984*, privacy advocates have invoked the image of English, utilitarian philosopher Jeremy Betham's Panopticon as another symbol of oppression. Based on Betham's model prison, and brought back into the historical consciousness by French philosopher and historian Michel Foucault, who was interested in using the Panopticon as a device to illustrate the levels of power in society, the symbol of the Panopticon has remained a powerful one.

Jeremy Bentham first penned the image of his model jail in 1787. Initially envisioned as a prison, the circular structure was to have cells on the outside of the wheel. At the centre lay the jailor, cloaked in darkness, but able to observe the prisoner at all times. The prisoners were to be isolated from one another and always under the gaze of the inspector. Within the Panopticon, the knowledge that one is being watched, but not knowing by whom or when, forces strict adherence to the rules. With the centre always in darkness, the prisoners always lit, the threat of constant repercussions was thought to be stronger than the desire of prisoners to circumvent laws. Here was a method to control behaviour and modify it to suit a set of goals, be it better discipline or work productivity. Bentham believed that the structure should be extended to asylums, factories, and schools, reasoning that few would break the law, or even stretch the boundary of convention, if one could not be certain that one was not being watched.[3] Bentham's model was impossible to implement then, and it does not seem any more reasonable in modern society. Nonetheless, the Panopticon has remained a compelling symbol for state oppression and abusive assertion of power through the total elimination of privacy.

While the Panopticon remains an interesting tool of analysis, much of the current literature concerning privacy suggests that power is outside of the state structure. Until very recently, it was thought that Orwell's centralized state, which kept tight control through surveillance and terror, was the system that had to be feared. Now, everyone from your local business Web site operators

3 Christopher Dandeker, *Surveillance, Power and Modernity. Bureaucracy and Discipline from 1700 to the Present Day* (Cambridge, 1990); David Lyon, *The Electronic Eye: The Rise of Surveillance Society* (Minneapolis, 1994); Michel Foucault, *Discipline and Punish. The Birth of the Prison* (New York, 1975).

to your next-door neighbour has the opportunity to impinge on your privacy. With personal video cameras, tracking software, and a proliferation of stores that sell spying equipment, the price of surveillance is affordable to all. The power, once held by the state has become dispersed, diffused, and harder to locate; consequently, it is more difficult to protect against it or to hold it to account. We have, as Reg Whitaker has suggested, moved from a "surveillance state" to a "surveillance society."[4] "In the waning years of the twentieth century, our technocratic societies can accomplish what George Orwell could only fantasize about in the aftermath of the Second World War," warns David Flaherty, former privacy commissioner for British Columbia and Canada's leading scholar on the topic.[5]

Privacy, along with the virtues of liberty, freedom of expression, and freedom of association, is usually held up as a major tenet of a democratic society. Loss of privacy, then, is often associated with the loss of democracy. These points are not simply abstract issues for academic debate. Privacy is important to individuals, and several surveys of Canadians have affirmed that importance. An Ekos Research poll of 3,000 Canadian households in 1993 found that "concern about privacy in Canada today is remarkably high." Ninety-two per cent of all Canadians expressed at least moderate levels of concern, and in relation to other topics, the fifty-two per cent who expressed "extreme" concern for issues related to privacy surpassed those concerned with national unity (thirty-one per cent) and virtually equaled concerns with unemployment (fifty-six per cent) and the environment (fifty-two per cent).[6] An overwhelming majority claimed that they wanted more control over how their personal information was to be gathered. Fears heightened as the millennium approached: a recent article in *Atlantic Monthly* cited a 1999 *Wall Street Journal*-NBC survey, which starkly revealed that Americans were more concerned with losing their privacy in the twenty-first century than they were with overpopulation, racial tensions, and global warming.[7] With the terrorist attacks of 11 September 2001, that fear has recently been superseded by issues of personal safety.

In this age of Internet communications and electronic commerce, it is becoming easier to collect information on an individual. Electronic commerce consists of computer-based transactions involving the processing and transmission of digitized information. Each transaction leaves a data trail. And

4 Reg Whitaker, *The End of Privacy: How Total Surveillance is Becoming a Reality* (New York, 1999), p. 29.

5 David Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States* (North Carolina, 1989), p. 6.

6 Ekos Research Associates Inc., *Privacy Revealed: The Canadian Privacy Survey* (1993).

7 Toby Lester, "The Reinvention of Privacy," *The Atlantic Monthly* (March 2001), p. 27. Also see, Andrew Petter, *A Discussion Paper: Protecting Personal Privacy in the Private Sector* (British Columbia, October 1999), pp. 2-3.

those trails can be gathered up, processed, and eventually brought together to say something greater about an individual person, than the sum of the once-scattered parts. There may not be a strong trail for a single credit card transaction, but a series of them, gathered together over a year, will tell something of the individual's purchasing habits. Add to that the growing use of debit cards, the digitization of health, education, and employment records and the audit trail of those browsing on the Internet, mailing in rebate forms, and entering give-away prizes at conventions, and a profile of each person begins to emerge. Big purchases like cars and houses which require mortgages and loans are other places where we must give significant personal information to others, to say nothing of enrolment in schools and universities, applying for any government grant or programme, or paying taxes at any level. None of this has gone unobserved by the media of course. It is not uncommon to read accounts like the one from the *National Post* which suggested that "Your deepest secrets are just a click away from becoming very public."[8] In a world of paper-based transactions and information seeking, the gathering of personal information was done too, but it could only be matched and linked with great difficulty, and only for a very few targeted individuals; now, with the linking of databases, the use of identity numbers, and the passing of trillions of megabytes over systems, it is much easier to mine data to create profiles on individuals.

The removal of geographical limitations combined with new technological convergence means that most of this information is gathered without contacting the individual. Personal information is amassed and potentially distributed without consent. In the new information-driven economy, there is money to be made in this form of commerce.[9] Businesses want to understand customers in order to better tailor products to meet their needs in the new "niche marketing" that now drives capitalism. In itself that is not a nefarious situation; indeed, it may lead to better services, rather than forcing consumers into a narrow set of choices. Yet the difference between tailoring business needs to accommodate clients and to discriminate against others is a precarious one. With such a breadth of information available about people and their habits, what is stopping an insurance company from denying coverage to some clients based on aspects of their medical history, or worse, on particular lifestyle?

Technology plays a large part in creating this unsettled feeling among citizens. There is now software that can make a digital image of your face, store it, and then link it to a real-time camera scanning a crowd. The manufacturers of one system claim that they can match faces to a database of fifty million in

8 Peter Goodspeed, "How much do they know?" *National Post Online* (28 February 2000).

9 Colin J. Bennett and Rebecca Grant, eds., *Visions of Privacy: Policy Choices for the Digital Age* (Toronto, 1999), Introduction.

less than a minute.[10] Certainly this has implications for freedom of association, which events such as the APEC protest in Vancouver or the 2001 Quebec City people's summit, have pushed further into the limelight. Of course, after the 11 September 2001 terror attacks, the likelihood is very high that the use of such technology will accelerate, especially in airports, train stations, cruise piers, or other high-volume areas of traffic. Yet it is a long reach from trying to catch murderers and known terrorists to surveilling legal democratic protest. What if the government could scan the crowd at a protest, save the image of anyone there, and then use it in future operations? If it is dangerous to protest these days, one should be very careful where you sit. A *Maclean's* article of 2001 noted that this technology, while scanning the tens of thousands sitting at the Superbowl last year, aided in the capture of at least two criminals.[11] Depending on the crimes, perhaps, many would applaud. Yet this is the slippery slope to losing personal freedom. Software that scans and links related images and data is becoming perilously close to the fiction portrayed in Hollywood movies like *Enemy of the State*, in which Will Smith played an innocent citizen who was tracked all over the United States by satellite cameras. Less futuristic, but more common in all societies, are security cameras. These help to provide a sense of personal and group safety, and most of us would support their placement in underground parking garages or in one-clerk convenience stores that are open late at night. But what happens when more cameras are introduced: cameras that track our actions at sporting events, cameras that give us speeding tickets, cameras in archival research rooms, cameras that place us under surveillance at all times? When do our actions as individuals become inhibited? When is our freedom compromised? The argument is that cameras help to catch criminals. But what will be their impact on the vast majority who are not criminals? I suggest that these intrusions on privacy are damaging to individuals and to society.

As a rule, the state, through its civil service and other agencies, is always gathering information about people. Routine gathering of personal information need not be immediately seen as infernal; it is simply the way large bureaucracies deal with the enormous task of tracking and serving millions of clients. It is the essential component of giving citizens their rights to health care, pensions, scholarships, passports, and a thousand other programmes and benefits. Data collected with proper care and within regulations is generally seen to be acceptable. Even the most diehard privacy advocate will acknowledge that personal information is required to run programmes, deliver services

10 Examples drawn from Bruce Phillips, "Privacy: The Newest and Oldest Human Right," The Seventh Dr. Bernie Vigod Memorial Lecture, 7 November 1996 and round table discussion, "Technology of Privacy or Technology of Surveillance?" in *Proceedings from Privacy & Information Technology: Friend or Foe?* (New Brunswick, privately published, 1997).

11 Chris Wood, "Do you Know Who's Watching You?" *Maclean's* (9 February 2001), pp. 18-23.

12 Andrew McIntosh, "Ottawa defends 'big brother' database," *National Post* (17 May 2000);

effectively, anticipate trends, plan programmes, and meet the requirements of individuals themselves. However, it is what the government and other agencies do with the information afterwards that many find so troubling. One need only recall the outcry when the media broke the story of the Department of Human Resource Development Canada creating a database with information on individuals. Accusations flew in the House of Commons, editorials decried the return of Orwell's Big Brother, and Canadians wrote to the government in the thousands demanding to know what information was being held on them. While privacy advocates were correct to demand the disbandment of this illegal database, the media coverage of the incident proved once again that privacy issues have the potential to make a strong impact in our society.[12]

In short, there is a growing sense of unease in society regarding technology that enables our personal information to be gathered and sold to the highest bidder, or to be misused by those with advanced computer expertise. Many people feel that regaining control over their personal information and protecting their privacy in the unregulated world of electronic commerce is essential even if they cannot articulate what it is that they want changed. Without knowing what personal information is being held by others, we are all relegated to being prisoners in the Panopticon. That has become increasingly unacceptable for many Canadians and it is clear that the federal government has heard and is responding to these concerns.

Government Action

In the 23 September 1997 Speech from the Throne, the Liberal Government outlined their plan for ensuring that Canadians would be in the forefront of the electronic revolution. Prime Minister Jean Chrétien expressed his desire to "connect" Canadians to one another and, in the process, become the "most connected nation in the world."[13] It had been clear for some time, though, that in building this new information economy and society, it was essential that consumers feel secure and comfortable, not only to use the new technology but also to have faith in it. To develop this trust, Chrétien advocated new legislation to protect personal information.

12 Andrew McIntosh, "Ottawa defends 'big brother' database," *National Post* (17 May 2000); "HRDC Dismantles Longitudinal Labour Force File Databank," *Human Resources Development Canada Press Release* (29 May 2000) at <http://hrdc.gc.ca/common/news/dept/00-39.shtml>; "Privacy Commissioner applauds dismantling of database," *Privacy Commissioner of Canada, Press Release* (29 May 2000), <http://www.privcom.gc.ca/media/nr-c/archive/02_05_b_000529_e.asp>.

13 Task Force on Electronic Commerce, Industry Canada and Justice Canada, "The Protection of Personal Information, Building Canada's Information Economy and Society," (January 1998), p. 1; Michael Binder, "E-Commerce Policy Briefing: Bill C-6 part of government's 'connecting Canadians' agenda," <http://www.thehilltimes.ca/briefs/e-commerce/agenda_e.html>.

As early as May 1996, Minister of Industry John Manley, on recommendations from the Information Highway Advisory Council, announced that legislation would be developed to protect personal information in the private sector. Information created or received by the federal government had already been relegated by the *Privacy Act* (1983) and the *Access To Information Act* (1983), but there was a pressing need to reign in the perceived loose privacy rules in the private sector. Most importantly, there was pressure to conform to new legislation in Europe.

In 1995, the European Union (EU) promulgated its *Directive on Data Protection,* which requires safeguards in the use of electronic personal information in the private sector. As well as setting guidelines for how personal information could be gathered and used, the directive required all member countries to meet pre-established standards by 1998. Article 25 of the *Directive* also prohibited member countries from sending and transferring such information to non-member countries that had not enacted similar laws protecting personal information from infringement. The motives driving the Canadian federal government are clearer if we understand that such legislation was necessary to ensure that Canadian companies did not violate article 25 prohibitions in *The Directive*: those in violation would be locked out of EU trade markets.[14] The Canadian bill was driven by economic and technological imperatives. There was little consideration for the impact of the legislation on the writing of history, on the integrity of archives, or, for that matter, on abstract notions of some fundamental right (as some allege) of personal privacy. While this ignorance of broader implication is not surprising, it did mean that archivists, historians, and journalists would have to press the government to ensure that their concerns were heard.

In January 1998, an Industry Canada discussion paper entitled, *The Protection of Personal Information: Building Canada's Information Economy and Society* was released. The paper urged the Canadian federal government to enact legislation that required the private sector to collect and share personal information in appropriate ways. From an archival and historical perspective, the enactment of the 1993 Quebec provincial legislation, *La Loi sur la protection de renseignements pesonnels dans le secteur privé*, was less than successful. Although welcomed by privacy advocates, it is so stringent in guarding privacy that it has the potential to launder archives and strangle history and heritage. In the rest of Canada, the Canadian Standards Association Model Code and the Uniform Law Conference of Canada's *Private Sector Protection of Personal Information Act* provide guidance to businesses on how to safe-

14 See *Bill C-6 : The New Meaning of "Private" for the Private Sector: Materials Prepared for the Continuing Legal Education Seminar, Bill C-6: The New Meaning of "Private" for the Private Sector*, held in Vancouver, BC on 1 June 2000 (Vancouver, BC, 2000) for further exploration of the EU Directive; and Michael Geist, "Battles brew as on-line privacy policies diverge," *The Globe and Mail* (3 May 2001), p. B17.

guard sensitive personal information. With the need to conform to the EU *Directive on Data Protection* and the growing apprehension among Canadians regarding their privacy, the government introduced Bill C-54 in Parliament on 1 October 1998.

Bill C-54 contained two major parts: Part 1, "Protection of Personal Information in the Private Sector," governed the collection, use, and disclosure of personal information in the private sector, and Part 2, entitled "Electronic Documents," provided guidelines for the use of electronic records for federal agencies that currently used paper to record or communicate information. Other parts of the Bill amended other federal statutes, including the *Canada Evidence Act*, in order to facilitate the use and legal recognition of electronic documents.

Debating Bill C-54

Between December 1998 and March 1999, the Industry Committee held hearings on Bill C-54. Sixty groups gave briefs and appeared before the committee, including federal ministers, the federal Privacy Commissioner, provincial Privacy Commissioners, public interest groups, privacy and constitutional experts, journalists' and writers' groups, and representatives of the business, insurance and health sectors. Although almost all of these individuals and organizations were concerned with the effect of the personal information legislation on their business practices, few submissions dealt specifically with archival and heritage issues. However, there was a small voice for archives among the cacophony demanding changes to the personal information components of the Bill. The Canadian Historical Association, the Association of Canadian Archivists, the Association des archivistes du Québec, and the Institut d'histoire de l'Amérique française feared that privacy legislation would affect the creation, preservation, and use of archival records for future generations of Canadians. They argued that it was necessary to include exemptions for historical research and the creation and maintenance of archives.

The four witnesses representing the archival and historical community were Joanne Burgess from the Institut d'histoire de l'Amérique française, Chad Gaffield, president of the Canadian Historical Association, Danielle Lacasse, president of the Association des archivistes du Québec, and Terry Cook, representative for the Association of Canadian Archivists. With industry driving the bill and privacy advocates pushing for stringent control, the original drafting of Bill C-54 contained few references to archives, history and culture. The archives group attempted to impress upon the committee the need to reconcile the right to protect one's personal information with the right to access to information. As it stood at that point, the drafters of Bill C-54 had failed to fully acknowledge the effect of this bill on archives; instead, all eyes were on issues of privacy.

It is evident from the transcript of proceedings that members of the Industry Committee were a little perplexed as to what these "historical types" wanted. It was useful, then, for the presenters to introduce who and what they were as professions. "As historians and archivists with a long tradition in handling personal information and the ethical issues it raises," explained Burgess, "our members are aware of the importance of protecting personal information."[15] In appealing to the notion of giving a voice to all Canadian citizens, Gaffield advocated that historians have understood the importance in writing about not only the great individuals and events of history but of society as a whole. Over the last four decades, history had become more inclusive and in order to ensure that there will be evidence to elucidate the lives of ordinary Canadians – the "history of the anonymous" – it was essential that records be kept so that future generations of historians could reconstruct and understand our collective lives, something that might not happen under the proposed legislation.[16] As Cook summed up in response to an inquiring question from the committee members: "I don't think I'm here just to argue, on behalf of archives, 'won't it be nice for our history and heritage'. I'm here to argue on behalf of Canadian society for electronic commerce and business itself, for government accountability, as well as for archives in history."[17] Cook explained that without core records appraised by archivists for long-term retention as a continuation of their original purposes, then business itself, government, advocacy watchdogs, and citizens would not have the sources necessary for analyzing long-term trends, for holding government accountable, for protecting citizen's rights, and for shaping our collective identities.

Despite raising the awareness of the archival issues, the archives group was but one of many to appeal to the committee. Nonetheless, they were able to effect some substantial changes. The archives group convinced the committee that personal information should be made available 110 years after birth, or twenty years after death. The committee had been wavering on how long to close records. The warning by the archives group that the 150 year closure stipulated by the Quebec privacy law had been far too stringent and was now being challenged in court, provided a clear example of privacy concerns overriding legitimate needs for access.[18] The Quebec example is particularly interesting since that province is so aware of the need to preserve and make available its own cultural heritage. Privacy legislation and heritage policy do not easily complement one another.

15 Standing Committee on Industry, *Record of Evidence* (hereafter Transcript), 18 February 1999.

16 Transcript.

17 Ibid.

18 Joanne Burgess, "The Right To Privacy in the Private Sector: What is at Stake for Historians and Historical Research," letter posted on 21 October 1998 to the Canadian Historical Association Web site.

At the same time, the archives group asked for the rewording of several phrases to sharpen the exclusion of archives to some of the blanket statements. Under the limits and exemptions of the Bill, section **4(2)(c)** noted that the legislation did not apply to "any organization in respect of personal information that the organization collects, uses or discloses for journalistic, artistic or literary purposes and does not collect, use or disclose for any other purpose." The archives group attempted to have section **4(2)(c)** amended to "explicitly exempt organizations operating solely within archival missions." Unfortunately, the final act did not reflect that wording. The archives group also attempted to change the clause in section **7(2)(c)** relating to use of data without consent. It states that personal information may be employed if "it is used for statistical, or scholarly study or research, purposes that cannot be achieved without using the information, the information is used in a manner that will ensure its confidentiality, it is impracticable to obtain consent and the organization informs the Commissioner of the use before the information is used." The archives group hoped to insert the phrase: "The use and disclosure of personal information for historical, statistical, or scholarly purposes is not deemed to be incompatible with the purpose for which it was collected." That clause would have made it explicitly clear that the use of information in archives is not a secondary purpose of the record and is, in fact, another component of the life-cycle of the records and its original purpose. This reflects the position of the European Union, perhaps because in Europe, the artificial distinction between active "records" and historical "archives" has never been as sharp as in North America. As it stands, section **7(2)(c)** recognizes the distinction between information used for commerce and that used for "scholarly study" – an important qualification; unfortunately, what is "scholarly" is open to some interpretation. However, that clause, if it is broadly interpreted in the courts, when combined with the exemptions in **4(2)(c)**, suggest that archives are largely outside of the most stringent requirements of the legislation.

In the second component of the Bill relating to electronic records, the archives group, strongly warned of the "fragile" nature of electronic records that can disappear at a key stroke or be unreadable after a couple of generations of software evolution. Of primary importance, Cook warned of the need to include de-encryption regulations. As e-commerce has become more prevalent, increasingly sophisticated software with more robust encryption encoding has been implemented to assuage the worries of the public, government, and businesses. Yet when these records are eventually transferred to archives, there will be no guarantee that anyone will be able to read them without the necessary decryption codes. In fact, it is likely that large amounts of information will be lost. Despite warnings that there would be "severe economic and legal chaos" if these electronic documents could not be decoded and used as reliable evidence in the courts of law, let alone later in the court of history, the Act did not acknowledge that de-encryption criteria were necessary to ensure

readability.[19] In fact, there were no changes to any other sections of the Bill, except those relating to privacy. Although members of the committee were sympathetic to issues of archives, memory, and history, they obviously felt constrained by the many pressures applied from other interest groups.

There were a number of amendments made to Bill C-54 at the committee stage, but the bill did not progress beyond report stage prior to prorogation of Parliament on 18 September 1999. However, the bill was reintroduced in the second session of Parliament as Bill C-6 and received Royal Assent on 13 April 2000.

The *Personal Information Act* and its Relevance to Archives

The act was promulgated in order to provide rules to govern the collection, use, and disclosure of personal information in the private sector. As a result, Part I of this Act only affects private-sector records. The implications of the Act for archives, however, are profound.

Pursuant to clause **4(2)**, Part I of the Act does not apply to **(a)** any government institution to which the *Privacy Act* applies and **(c)** any organization in respect of personal information that it collected, used or disclosed for journalistic, artistic or literary purposes and did not collect, use or disclose for any other purpose'. **4(2)(c)** is an important clause but it is qualified by a number of factors in section seven. During the committee debate in 1998, the archives group hoped that section **4(2)(c)** would be amended to "explicitly exempt organizations operating solely within archival missions." This was not done nor was the phrase "scholarly research" included in the list of exemptions that read "journalist, artistic, or literary purposes."

There appear to be three issues in Part I that directly affect archives: the capture and creation of records, the use and then the disclosure of them. It seems quite likely that many commercial entities will no longer be creating certain types of records. Very few people are ever likely to read the Act, and most will know only that they or their business are now prohibited from creating personal information clusters – be they compiled records or data banks – for use outside their original, primary purpose. How deeply this will affect archives is unknown, but it will likely result in fewer and poorer records being transferred to archives. If data of this type must be destroyed after it is used, these records will never make their way to archives. The destruction of records containing personal data could also be extended to other records and that remains a disturbing thought.

While the archives group attempted to have a clause inserted that clearly stated that "The use and disclosure of personal information for historical, statistical, or scholarly purposes is not deemed to be incompatible with the pur-

19 Transcript.

pose for which it was collected," it appears that the spirit of such a statement was included in section **7(2)(c)**. There is a clear distinction that information for commercial uses is subject to the Act, but that information may be used "without knowledge or consent of the individual" if "it is used for statistical, or scholarly study or research, purposes." John Manley, the Minister of Industry, spoke at the Senate Committee studying Bill C-6 on 2 December 1999 and reiterated that the bill was about balancing commerce and privacy. Nonetheless, during that address, he said the bill recognized the "fundamental right of free speech in an exemption for journalistic, artistic, and literary expression." He finished his remarks by suggesting that the goal of Bill C-6 was to "establish in law a right to privacy without: placing an undue burden on business; intruding on the right of freedom of expression; or destroying our historical memory by interfering with the preservation of documents."[20] His comments and the qualifications in the final Act suggest that the role of history and archives were recognized as a legitimate concern, and articulated with clear exemptions. The spirit of the Act suggests, and will hopefully be confirmed through practice and the courts of law, that historical records are important and should be used and disclosed by archives and their stakeholders.

It is interesting to note that the 1995 European Union *Data Directive*, which initially forced the Canadian federal government to devise privacy legislation for the private sector, also states that the "processing of personal data for historical, statistical or scientific purposes is not generally to be considered incompatible with the purposes for which the data have previous been collected." Providing there are "suitable safeguards," then, the European parliament has judged archives to be a part of a continuum.[21] This is also a consideration in the Canadian federal *Privacy Act* that allows for the transfer of material and information to the National Archives, for statistical or scholarly work, although subject to various regulations. If this continuum concept was accepted in Canada, we would have far fewer problems to worry about in regard to privacy issues.

There is more to Part I, much of it centreing on the mechanics of resolving grievances and the role of the Privacy Commissioner, who is assigned the task of enforcing the Act. There are further nuances to the Act, and for those interested or affected, it will be necessary to delve more closely into the complex constructions of legal writing.

The Act has another major component to it: Part II which applies to electronic documents and Part III which relates to amendments to the *Canada Evidence Act*. Although discussion of these parts are outside the scope of this article on privacy and archives, there is a synergy with Part I which is not

20 Testimony by John Manley before the Senate Committee Studying Bill C-6, 2 December 1999, <http://www.connect.gc.ca/en/sp/1328-e.htm>.

21 Directive 95/46/EC of the European Parliament, Section 29.

apparent at first glance. Part II and III of the Act are important insofar as they give sustained attention to the growing importance of electronic records as part of the business function of all agencies and organizations.

The Act suggests the necessary characteristics of a reliable electronic record. By modifying the *Canada Evidence Act* and decreeing that electronic records are to be on the same legal footing as paper ones, and that they may be presented in court as the "original" record, the Act has important ramifications. Yet for a record to be given due weight as evidence in a court, the user must be able to prove the "integrity of the electronic document."[22] With these stipulations, then, record-keeping must change to better document how records are created, kept and accessed. If records are to be used in court, there must be safeguards to ensure their authenticity. The Act indicates that it is incumbent on the individual or organization to prove that electronic records have not been altered or tampered with, meaning that electronic signatures and secure record-keeping systems are necessary. This will result in all records managers being forced to tighten control over record-keeping systems, with standards and procedures being documented, metadata elements provided, and all changes to records tracked and discerned through identifiable work processes. Encryption will also be used increasingly. If electronic records are to be used in court as trustworthy evidence, government and businesses must have better record-keeping systems than they presently do. Although the changes to the Evidence Act may not entirely reverse the trend in starving records managers of resources, it should provide some much needed ammunition in the fight to exert better control over records management. And that should eventually equate into better-managed records being transferred to archives.

Clio vs. Big Brother

It is clear that we do not want an Orwellian world where citizens are under constant surveillance and where powerful corporations or intrusive governments know everything about our lives. But overreacting to the threat of privacy infringements also runs the risk of wiping out our collective history and heritage. Does the passing of the new legislation threaten the death of history? No, of course not. In most cases, the large databases of personal information from commercial transactions do not constitute the only source of information about Canadians; moreover, much of this type of information is usually not appraised as being archival. While there is a need to strike a balance between the individual's right of privacy with society's need for a collective memory, it

22 For a discussion of these issues, see Ken Chasse, "Electronic Business Records in Legal Proceedings," ARMA International Conference, 10 April 2001. Readers will be struck by the similar wording and ideas that correspond to InterPARES documents, available at www.InterPARES.org.

is imperative that archivists have the opportunity to appraise the fullest records for their values rather than assessing only what is left after companies or individuals destroy records according to privacy legislation.

There are other less tangible issues that present concern. Does this legislation indicate a sea-change in the thinking of the public? Will such legislation, which is almost never read and rarely understood, have a chill-factor impact on decisions to create fewer or different kinds of records? Will individuals begin to systematically destroy their records in order to protect themselves and their institution, simply in order to avoid the trouble, cost, and potential embarrassment of being taken to court?

Executives in the private sector will more likely be avoiding litigation rather than thinking about how their records might document history or complement archival holdings. If destruction is the key then – and it is the approach advocated by the Privacy Commissioner – one wonders and worries about how far this will embed itself into the consciousness of individuals. There are no laws in Canada that govern the preservation of private-sector records such as those for government records under the *National Archives of Canada Act* (1987) or under most provincial archives legislation. Could we understand the twentieth century with only government records and without private archives like diaries, letters, photographs, and videos of everyone from prime ministers to great war soldiers, from labour organizations to school teachers? What about important business fonds like Dominion Textile Inc., whose records not only thoroughly document Canada's textile industry, but also shed light on labour-management relations, and the lives of the working-class. The records of the Ontario and Quebec Paper Company, a pulp and paper mill that had operations in Thorold, Ontario and Baie Comeau, Quebec, are equally rich in documenting our past. The company was actually a Canadian spinoff of the *Chicago Tribune* newspaper, and its records reflect the issues and concerns of Canadian subsidiaries. Need one discus the value of the fonds associated with Molson, Brascan, or Polysar?

Privacy advocates urge us to be diligent to prevent the further erosion of personal privacy. The control of personal information for them boils down to one word: consent. Without consent, you cannot reuse information. This seems wholly sensible for insurance companies or telephone marketers who have been more likely in the past to reuse client information for unintended and unauthorized secondary purposes. The problem, of course, is that almost all information in archives consist of "secondary value" information. Records are created for one purpose and then used for quite another. The result has been the transfer, presentation, and use of vast stores of records in archives for purposes radically different than their original reason for being created. Negotiating a legal requirement for consent to archiving when data is collected, then, is a very difficult and thorny issue. It is absolutely necessary for businesses, but it proves a dilemma when applied to scholarly, historical purposes.

A legal requirement for consent applied at the lowest level might very well destroy how archives do their work of preserving and making available historical documentation.

In 1993, Bruce Phillips, the Canadian Privacy Commissioner, responded to thirty citizens who complained that the 1991 census was an intrusive threat. He claimed that the secondary use of these records – for historical, cultural, or social purposes rather than for the stated reasons behind taking the census, such as counting Canadians, delineating federal electoral districts, calculating transfer payments, or providing anonymous statistical data for all manner of public policy issues – was not explained in the questionnaires. To release that information without the signed consent of each census respondent would therefore be an unacceptable invasion of privacy. Phillips demanded that all personal information be expunged; in effect, leaving only the aggregate data, and all but rendering the "historical" nature of the census useless. Reacting to these concerns, Statistics Canada's solution has been to mollify the opposition by forever locking the information away or volunteering to destroy the record. Why stop there? Why not destroy every record containing personal information: immigration registration, artists' grants, medical records, native band lists, and on and on. This is the Privacy Commissioner's solution and one which the National Archives of Canada, along with numerous historically-minded groups, have strongly opposed.[23]

Heather MacNeil has written that consent is necessary if we are to keep that sacred bond between archivists and donors.[24] Yet informed consent is impossible to achieve. There would have to be pages of appended information describing how the personal information is closed for decades before release; or how historians and genealogists, possibly an individual's decedents, needed that data to reconstruct the past. The logistics of gathering and using the consent of millions would be prohibitively burdensome. At the same time, it seems clear, with the Canadian *Bill of Rights* and the increased focus on individual and human rights, confirmed again and again in courts of law, that history has taken a backseat to privacy issues, when these are couched in terms of "personal rights." The most effective response for archivists to this dilemma may be in the idea of consistent use.

Privacy advocates argue that consent should be kept at the lowest level, with the individual. Archives are uniquely positioned to be more forceful in arguing that consent should be applied at a higher level and that it is intertwined with records creation. From an archival perspective, the retention and archival use of records is consistent with their creation and original adminis-

23 See Jean-Stéphen Piché and Sheila Powell, "Counting Archives In: The Appraisal of the 1991 Census of Canada," *Archivaria* 45 (Spring 1998) for more details on this ongoing battle.

24 Heather MacNeil, "Defining the Limits of Freedom of Inquiry: The Ethics of Disclosing Personal Information held in the Government Archives," *Archivaria* 32 (Summer 1991).

trative use, and forms part of the records continuum. This does not mean that archives would flaunt public concerns about privacy, especially over sensitive personal information, but simply that as part of the records continuum process, individuals and the government would acknowledge that where records were deemed archival, they could not be destroyed simply because of privacy concerns. As privacy advocates begin to demand stronger measures, it seems clear that archives and their champions must convince legislators of the importance of seeing records as part of a continuum.

While the nightmare of twentieth-century persecutions and conflict is still indelibly imprinted on our collective memories, there is every right to think that people would and perhaps should ask to have information on themselves restricted or destroyed. Putting aside the fact that the information in exceptionally rare cases could be wielded against a person fifty or sixty years later, what is of the greater good to society? Is it morally right to say that we must protect ourselves absolutely and therefore destroy everything that relates to us? This is what the Privacy Commissioner is implying regarding the census. Based on some thirty complaints, most of which related to having neighbours supervise the survey and therefore having access to personal information, this reaction appears to be blown out of proportion.[25] A brief of the Canadian Historical Association to the Expert Panel on Access to Historical Census Records pointed out that although Canadian census material was open up to 1901, there had not been "a single word of protest from any Canadian over the violation of their privacy."[26] More recently, the opening of the 1901 census for England and Wales was so anticipated, that during the first day the information was available, the Public Records Office's Web site crashed as more than 1.2 million users tried to access material. With over 100,000 Web sites devoted to genealogy, it is clear that history, especially individual, personal history, matters to a great many Canadians and citizens throughout the world.[27] Not surprisingly, then, the Federal Privacy Commissioner's attempt to have the Canadian census culled of all personal information has caused a tidal wave of opposition from historically-minded and genealogical groups stressing the need for records that promote openness and accountability, while providing evidence of past deeds and actions to know both our country, our community, and ourselves. To destroy records that underpin such values is morally wrong, misguided, and in the long run contrary to our very ability to know ourselves and our society.

It is not simply the census that is in danger when we allow individuals to decide on consent or if we give way to our collective unease surrounding pri-

25 Transcript.

26 Canadian Historical Association Brief to the Expert Panel on Access to Historical Census Records, 9 February 2000, p. 5.

27 For the 1901 census and genealogical Web sites, see Owen Gibson, *Guardian News Service* (2 January 2002); and Richard Starnes, *Ottawa Citizen* (3 January 2002), located at: <http://www.nationalpost.com/news/world/story.html?f=/stories/20020103/1020877.html>.

vacy issues. To use examples from federal records, both the Japanese-Canadian redress for their forced evacuation during the Second World War, or the many cases of Aboriginal injustice, from the removal of children from their families to abuse in residential schools, reveal the danger of destroying records that contain personal information. What would have been the answer in early 1942 (or anytime), if a government agent had been required to ask a citizen for consent to keep records of impounding their boat or other property, the forced sale of their house below cost, or the removal of their child from the family – all for the benefit of the nation's archives – the same nation and government that was at that moment inflicting harm on them, the citizen? One can imagine that very few, if ever given the choice, would consent. Yet, ironically, it is these exact records that have been used by Aboriginal Canadians, Japanese Canadians and others to redress some of the injustices of the past.[28] Now, with the aid of hindsight, it is clear that such records have value both to the individual and to society as a whole. It has been said that historians are very good at predicting the past. But no one can predict the future. We simply do not know which records will be of use in the future as evidence in courts of justice, to protect citizens' rights, or hold officials to account for abuse of power. Of course we cannot keep every record, but we must at least allow the eventual guardians of those records – archivists – to appraise them, and retain the small fragment they deem to have archival value.

Perhaps Orwell, who has provided so much material for privacy advocates, is instructive in other ways as well. In trying to protect ourselves against Big Brother, we might unwittingly be playing into the hands of Orwell's other equally terrifying spectre: the Ministry of Truth, which rewrites history to fit the latest need of the state. If we demand that certain records with archival value be destroyed – for whatever reason – are we not advocating, indeed embracing, the potential for Orwellian truth-twisting? For without authentic records, we are in danger of abusing the past.[29] We must not allow ourselves to be seduced by the flawed logic that destroying records that document personal information will protect individuals. It will not. That process of unfettered destruction will only help to diminish our understanding of each other and of our society. Deny a citizenry its history, even parts of it, and you begin to deny them the chance to make informed choices, to understand themselves, and to question the government, now and in the future.

The key, of course, is finding a balance between protecting privacy and access to information. Archives are not, and do not aspire to be, Jerry

28 Interview with Dr. Terry Cook, 15 June 2001. Also see Judith Roberts-Moore, "The Office of the Custodian of Enemy Property: An Overview of the Office and its Records, 1920-1952," *Archivaria* 22 (Summer 1996), pp. 95-106.

29 See Verne Harris, "Redefining Archives in South Africa: Public Archives and Society in Transition, 1990-1996," *Archivaria* 42 (Fall 1996), for a contemporary analysis of these problems as found in South Africa.

Springer-like shows, getting the "goods" on people to embarrass them. However, archives have a duty to all Canadians to document their society. To argue that it is better to destroy information rather than allow it to be used sometime in the future, often a lifetime away from the present, is to deny a collective self-consciousness to millions of Canadians who will never be famous for playing hockey, for writing books, or for leading parliamentary debates. Do we want a society that only remembers those at the top or those with a self-conscious eye on history? We must not allow those without a voice, even if they desire it at the time, to be silenced. There must be a balance between the right to information and the right to privacy, between the right to redress injustices in the future (which of course can never be predicted) and the present concerns of individuals for privacy, between the legitimate need for temporary protection of personal information and the long-term need to understand our collective heritage.

Conclusion

Most records created in society and that fall under the domain of archives, will not be directly affected by the new *Personal Information Act*. Certain types of business and labour records are the exception. That seems to be the spirit of the Act at least. However, the indirect effect on record-keeping and the sea-change attitude that may be provoked by the Act may very well result in the destruction of many other types of private records. This Act may be an impetus to further the tendency of businesses and individuals to purge records. Equally troublesome is the larger conflict between archives and privacy. The government is planning to rework and rewrite the federal *Access to Information Act*. Will the federal *Privacy Act* follow? Recent court cases over the right to photograph an individual in a public place or the question of whether privacy rights can be passed on to heirs should be a concern to all archivists. Is our society so worried about privacy infringement that we are willing to sacrifice our culture in the process? One hopes not. Certainly the ramifications of such actions need to be explained, with keepers of heritage and history countering the arguments of those who advocate the pre-eminence of privacy.

There is, without a doubt, a fight brewing on the horizon. It will pit privacy against archives and history, with their champions in the front lines. And right now it appears that privacy advocates are better positioned in this struggle. It is much easier to argue against any erosion of privacy, and to draw on all the symbols of repression, both real and imagined, than it is to plead for the importance of archives and all the intrinsic value that they connote. Privacy is personal and immediate; culture (and history) is abstract and long term.

Citizens must be guaranteed that their personal lives are not an open book. At the same time, archivists must also ensure that citizens have a right to know about their government and their collective identities and heritage. The

Personal Information Act will be used by both sides, to help strengthen their arguments. Without a doubt, the electronic records component of the Act (Parts II and III) will assist in records management and will help to promote more openness and accountability in government. Unfortunately, it also seems clear that the privacy component (Part I) will hinder some archives and likely result in the destruction of certain types of records. Nonetheless, by joining together the several parts of the initial Bill C-6, it appears that the government is concerned with the long-term preservation of records. The seeming exclusion of archives from the full force of the Act is a welcome indication of that historical awareness. As then Minister of Industry, John Manley, the driving force behind the Bill, made clear, this new Act was not meant to hinder historians and fellow Canadians attempting to understand their collective past. Quite the opposite. There is a recognition of the continuum thinking inherent in the electronic records component of the Act, in so far as there is a continuous need for records as evidence. It is not difficult to see how this could also be extended to all archival records.

With privacy advocates focussed on the potential for government and business transgressions against our collective privacy rather than on the needs of individuals, society, and history for accountable results of government and business actions, archivists cannot sit on the sidelines and hope that good records will somehow survive. Like the archives group that presented to the Parliamentary Committee, we must get involved and make sure the archival voice is heard and understood. For without it, the archives of the future may very well consist of little more than state records, great people, and great silences.

This is not simply an academic debate, as the fight over the census makes clear. Archives are in danger and archivists will have to champion the right for all Canadians to have access to our collective history and identity, and ensure that in the process of protecting against Big Brother, we do not end up killing Clio and supporting many Ministers of (Un)Truth. That in itself would be a crime perpetrated against all Canadians, those from our past, those living, and those not yet born.